(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С ДОГОВОРОМ О ПАТЕНТНОЙ КООПЕРАЦИИ (PCT)

(19) ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
Международное бюро

ВОИС

PCT

(43) Дата международной публикации:
24 Декабря 2003 (24.12.2003)

(10) Номер международной публикации:
WO 03/107583 A1

(51) Международная патентная классификация [7]:
H04L 9/00, G06F 17/60, G06K 19/073

(21) Номер международной заявки: PCT/RU03/00266

(22) Дата международной подачи:
18 июня 2003 (18.06.2003)

(25) Язык подачи: русский

(26) Язык публикации: русский

(30) Данные о приоритете:
2002116399 18 июня 2002 (18.06.2002) RU

(71) Заявитель и
(72) Изобретатель: **ГЕРТНЕР Дмитрий Александрович** [RU/RU]; 167000 Сыктывкар, ул. Горького, д. 9, кв. 20 (RU) **[GERTNER, Dmitry Alexandrovich**, Syktyvkar (RU)].

(74) Агенты: **ЕГОРОВА Галина Борисовна, МИЦ Александр Владимирович, ООО «Юридическая фирма ГОРОДИССКИЙ И ПАРТНЁРЫ»**; 129010 Москва, ул. Б.Спасская, д. 25, строение 3 (RU) **[EGOROVA, Galina Borisovna, MITS, Alexander Vladimirovich, «GORODISSKY & PARTNERS LAW FIRM» Ltd.**, Moscow (RU)].

(81) Указанные государства *(национально)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZM, ZW.

(84) Указанные государства *(регионально)*: ARIPO патент (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), евразийский патент (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), европейский патент (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), патент OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Опубликована
С отчётом о международном поиске.

В отношении двухбуквенных кодов, кодов языков и других сокращений см. «Пояснения к кодам и сокращениям», публикуемые в начале каждого очередного выпуска Бюллетеня PCT.

(54) Title: INDIVIDUAL CRYPTOPROTECTIVE COMPLEX

(54) Название изобретения: ПЕРСОНАЛЬНЫЙ КРИПТОЗАЩИТНЫЙ КОМПЛЕКС

(57) Abstract: The invention relates to information protection and user identification. Said invention makes it possible to extend functional capabilities including information encryption and decryption, electronic document authentification using an electronic digital signature, electronic documents protection against copying, exchange of electronic documents protected against copying, payment with the aid of electronic payment instruments and software and database protection against unauthorised copying. The inventive individual cryptoprotective complex comprises a code carrier in the form of a cassette for cryptographic data protection and a terminal device for communicating with peripheral devices such as a personal computer, a telephone and a card reader. The cassettes for individual cryptoprotective complexes are embodied in such a way that they have a unified architecture, common software and identical secret mother code. The cassette protective case is provided with light-reflective surfaces. Software for controlling the integrity of the protective case destroys the mother code in case of hacking. A data processing software checks input open information with respect to service digits which are used as a most important tool for carrying out different cryptographic operations. Individual data of a user including the electronic digital signature thereof is recorded in the personal protective device. The inventive cryptoprotective complex comprises a device for user identification in the form of an identification wristband which stores single-use access passwords.

WO 03/107583 A1

[Продолжение на след. странице]

(57) Реферат: Изобретение относится к области защиты информации и идентификации пользователя. Технический результат заключается в расширении функциональных возможностей, включая шифрование и дешифрование информации, аутентификацию электронных документов с использованием электронной цифровой подписи, защиту электронных документов от копирования, обмен электронными документами, защищенными от копирования; расчеты электронными платежными средствами; защиту компьютерных программ и баз данных от несанкционированного копирования. Персональный криптографический комплекс содержит носитель кода – кассету для криптографической защиты информации, и терминальное устройство для связи с внешними устройствами – персональным компьютером, телефоном, устройством считывания с карт. Кассеты персональных криптозащитных комплексов имеют единую архитектуру, общее программное обеспечение и одинаковый секретный материнский код. Защитная оболочка кассеты имеет светоотражающие поверхности. Программа контроля целостности защитной оболочки при попытке несанкционированного доступа уничтожает материнский код. Программа обработки информации проверяет входящую открытую информацию на наличие в ней служебных символов, являющихся важнейшим инструментом при совершении различных криптографических операций. В ПЗУ записывают персональные данные пользователя, включающие его электронную цифровую подпись. В состав персонального криптозащитного комплекса входит устройство идентификации пользователя – идентификационный браслет, служащий для хранения одноразовых паролей доступа.

ПЕРСОНАЛЬНЫЙ КРИПТОЗАЩИТНЫЙ КОМПЛЕКС

Область техники

Изобретение относится к области обеспечения защиты информации и предназначено для хранения кодов доступа, ключей и паролей, для идентификации пользователя, для безопасного обмена информацией по открытым каналам связи, для безопасного проведения различных расчётов электронными деньгами и их суррогатами, для заключения электронных сделок и формирования электронных документов, подтверждаемых электронными подписями без использования асимметричных ключей, для защиты компьютерных программ и баз данных от несанкционированного копирования, для безопасной передачи и обмена электронных документов с защитой от копирования.

Предшествующий уровень техники

Широко известны устройства идентификации пользователя с помощью пластиковой карты, содержащей микрочип, и кода доступа, вводимого пользователем для доступа к защищённым объектам. Недостатком является необходимость каждый раз вводить код доступа, а в случае, если карта предназначена для доступа к различным объектам, не связанным между собой, то пользователю необходимо помнить несколько различных кодов доступа.

Известно также устройство для безопасного хранения информации на кристалле, в котором объединены микропроцессор, шины, и память. Недостаток такого решения состоит в том, что с помощью специального электронного щупа можно отсканировать информацию с кристалла. Также могут быть использованы атаки, основанные на разрушении аппаратных устройств хранения данных лазерным лучом и методе ионного анализа.

Известны системы шифрования с помощью асимметричных ключей, основанные на использовании секретного и публичного ключей, а также на трудности инвертирования односторонних функций. Недостатком таких систем является то, что объём криптограммы значительно превышает объём исходной информации. К недостаткам также можно отнести постоянно снижающуюся криптостойкость данных систем вследствие создания быстродействующих ЭВМ, объединяемых в сеть и математических методов, облегчающих процесс дешифрования, а увеличение длины ключа, с целью повышения криптостойкости алгоритма, приводит к замедлению процессов шифрования и дешифрования и требует использования значительных вычислительных мощностей.

Известны системы шифрования с помощью симметричных ключей, основанные на методах многократной замены и перестановки элементов информации. Недостатком таких систем является необходимость обмениваться секретным ключом перед сеансом криптозащитной связи, вследствие чего возможен их перехват. Кроме того, зная фрагмент исходной информации и его криптограмму, легко вычислить ключ, а увеличение длины

ключа, с целью повышения криптостойкости, приведёт к замедлению процессов шифрования и дешифрования. Другой существенный недостаток такой системы шифрования состоит в том, что если более двух пользователей обладают ключом, то расшифровать информацию, предназначенную одному пользователю, смогут все обладатели ключа.

Известен способ аутентификации электронных документов путём его хеширования и шифрования значения хеширования с помощью секретного ключа лица, подписавшего документ, и дешифруемого открытым ключом данного лица. Недостаток такого способа заключается в том, что для идентификации электронной подписи пользователь должен знать, что открытый ключ действительно принадлежит лицу, от имени которого подписан документ. Кроме того, для идентификации даты подписания документа необходимо осуществлять сертификацию даты через специальные центры сертификации посредством сети Интернет. Применение электронной подписи требует организации доверительного удостоверяющего центра.

Известно устройство, представляющее собой смарт-карту, содержащую микрочип, используемую для расчётов путём проведения транзакций с использованием линий связи. Недостатками данного устройства и основанного на нем способа расчета являются: необходимость постоянного участия банка во всех операциях пользователя смарт - картой, что требует наличия сети терминалов, подключённых к линиям связи; пользователю каждый раз необходимо вводить свой pin-код, а для расчётов через Интернет пользователь вынужден сообщать его продавцу. Пользователи не могут производить расчёты между собой напрямую. Банк может отслеживать все операции пользователя смарт - картой и его местонахождение на момент совершения операции.

Известен способ использования асимметричных систем шифрования для расчётов электронными наличными деньгами: электронными банкнотами и монетами. Недостаток данного способа в том, что одна и та же электронная банкнота или монета может быть потрачена несколько раз. Электронная монета может обращаться ограниченное количество раз, так как в целях безопасности на ней записываются данные всех её прежних владельцев. Так же в целях безопасности банки ограничивают использование суммы электронных наличных денег на одной смарт - карте.

Известно устройство, представляющее собой электронный ключ, содержащий микрочип, в котором записан код доступа для пользования компьютерной программой, предназначенный для защиты программы от незаконного копирования. Недостаток данного устройства в том, что электронный ключ предназначен только для одной программы; кроме того, существуют методы создания эмуляторов электронного ключа, что позволяет несанкционированно копировать компьютерные программы.

Наиболее близким аналогом является система распределённых ключей на основе интеллектуальных криптографических плат PC Cards, включающих в себя защитное клеймо, микропроцессор и энергонезависимую память, в которую записаны ключи, уникальные для каждой платы. Микропроцессор осуществляет шифрование и дешифрование по алгоритму, записанному в памяти платы. Для осуществления криптографических операций плата вставляется в специальный разъем в компьютере, после чего пользователь вводит свой пароль и свои идентификационные данные, которые дают доступ к плате. Затем пользователи обмениваются открытыми ключами и вырабатывают временный симметричный ключ сеанса связи, который может быть динамическим, с помощью которого и осуществляется шифрование и дешифрование информации. Основной недостаток данных систем заключается в том, что плата не может определить, с каким объектом установлена криптозащитная связь, так как пользователь может воспроизвести алгоритм работы PC cards на обычном компьютере, а в качестве ключей пользователь может использовать набор случайных чисел необходимого размера, так как ключи, записанные в PC cards одного пользователя, не известны PC cards других пользователей, и подмену ключей определить невозможно. Вследствие данного недостатка, PC cards не могут использоваться для выполнения разнообразных функций, основанных на доверии к источнику информации. Кроме того, платы PC cards не обладают достаточно надёжной физической защитой от сканирования информации с кристалла.

Раскрытие изобретения

Задачей настоящего изобретения является создание многофункционального, универсального криптозащитного комплекса, удобного в применении, недорогого в изготовлении, имеющего высокую степень физической и логической защиты и высокую скорость обработки данных. Технический результат, достигаемый изобретением, заключается в расширении функциональных возможностей криптозащитного комплекса, который обеспечивает эффективное выполнение таких функций, как шифрование и дешифрование информации при её передаче от одного пользователя другому; шифрование и дешифрование электронных документов с использованием пароля дешифрования с возможностью дешифрования любым пользователем персонального криптозащитного устройства, знающим пароль дешифрования; шифрование и дешифрование электронных документов с защитой от навязывания ложной информации и внесения изменений; аутентификация электронных документов путём подписания электронной цифровой подписью пользователя; идентификация пользователя; защита электронных документов от копирования по аналогии с документами на бумажном носителе, имеющими защиту от подделки; возможность одновременного обмена электронными документами, защищёнными от копирования; возможность одновременного подписания электронного документа электронными подписями различными пользователями; расчёты электронными наличными деньгами и электронными векселями между различными

пользователями; возможность конвертации электронных наличных денег и электронных векселей в электронные деньги различных платёжных систем; защита компьютерных программ и баз данных от несанкционированного копирования.

Указанные результаты в соответствии с изобретением достигаются сочетанием устройств и способов, объединённых в персональном криптозащитном комплексе, состоящем из носителя кода - кассеты, с помощью которой осуществляется криптографическая защита информации, и терминального устройства, посредством которого осуществляется связь кассеты с внешним миром. Кассета имеет порт ввода/вывода открытой информации и порт ввода/вывода зашифрованной информации, которыми подключается пользователем к терминальному устройству с аналогичными портами. Терминальное устройство может быть соединено с персональным компьютером, с телефоном, с устройством считывания с карт. Одна кассета подключается к другой кассете посредством терминальных устройств и линии связи через порт ввода/вывода зашифрованной информации. Информация от пользователя и для пользователя передаётся соответственно через порт ввода/вывода открытой информации.

Кассеты всех персональных криптозащитных комплексов имеют единую архитектуру, общее программное обеспечение и одинаковый секретный материнский код , представляющий собой множество случайных чисел (M1, M2,...,MN) записанных в упомянутые устройства защищённым способом, исключающим возможность копирования материнского кода на другие носители и изменения программного кода программного обеспечения. Программное обеспечение и материнский код должны записываться в память кассет специальными записывающими устройствами, работающими в автономном режиме, к которым невозможен доступ извне, а материнский код, на основе которого устанавливается криптозащитный сеанс связи, должен формироваться с помощью аппаратного генератора случайных чисел непосредственно в центральном записывающем устройстве. Программное обеспечение записывается в ПЗУ кассеты, а материнский код записывается в энергозависимую память типа CMOS, питающуюся от встроенной аккумуляторной батареи. От данной батареи также питаются встроенные не настраиваемые часы реального времени, играющие важную роль в ряде операций, и защитная оболочка, в которую упакована кассета, предотвращающая извлечение из кассеты информации, содержащей данные материнского кода.

Защитная оболочка состоит из внешней оболочки корпуса, внешней светоотражающей поверхности, внутренней светоотражающей поверхности, прозрачного слоя, находящегося между светоотражающими поверхностями. Обе светоотражающие поверхности и обращены друг к другу. На внутренней светоотражающей поверхности расположены излучающий светодиод и несколько фотоэлементов. Программа контроля целостности защитной оболочки, входящая в состав программного обеспечения, контролирует подачу энергетических импульсов от аккумуляторной батареи к светодиоду и получение энергоинформационных импульсов с каждого фотоэлемента, и в случае изменения характеристик энергоинформационных импульсов

производит уничтожение материнского кода. Для выполнения операций в состав кассеты входит микропроцессор, ОЗУ, генератор случайных чисел. Для записи информации кассета снабжена многократно перезаписываемой ППЗУ. В состав программного обеспечения, записанного в ПЗУ, входит программа шифрования/дешифрования, программа обработки информации, индивидуальный номер персонального криптозащитного комплекса. Особенность программы шифрования/дешифрования состоит в том, что знание исходной и зашифрованной информации не влечёт за собой представления об использованном ключе – материнском коде, а шифрование любой информации производится с использованием по меньшей мере одного случайного числа, генерируемого перед началом шифрования встроенным генератором случайных чисел. Особенность программы обработки информации заключается в том, что программа проверяет входящую открытую информацию на наличие в ней определённых наборов бит, так называемых служебных символов, и при нахождении данных символов в сфальсифицированном электронном документе не допускает их включение в зашифрованный электронный документ. Включение в зашифрованный электронный документ служебных символов является исключительно прерогативой программы обработки информации. Служебные символы являются важнейшим инструментом при совершении различных криптографических операций, которые позволяют определить в электронном документе служебную информацию. Кроме того, функции программы обработки информации закрыты для пользователя, поэтому некорректные с точки зрения программы команды пользователя игнорируются, в то время как команды, поступившие в составе служебной информации, всегда принимаются программой к выполнению. В ПЗУ также записываются персональные данные пользователя, включающие его электронную цифровую подпись. Данная запись производится после приобретения пользователем персонального криптозащитного комплекса, причём запись производится официальным регистратором с одновременным занесением этой информации, включающей индивидуальный номер персонального криптозащитного комплекса, в открытую базу данных.

Дополнительно в состав персонального криптозащитного комплекса входит устройство идентификации пользователя – идентификационный браслет, снабжённый защёлками с датчиками фиксации, поводком для подключения к терминальному устройству и устройством для автоматической замены аккумулятора. Идентификационный браслет служит для хранения одноразовых паролей доступа, которые автоматически удаляются при снятии браслета, и обеспечивает удобную и быструю идентификацию пользователя при совершении им криптозащитных операций.

Краткое описание чертежей

Предлагаемая группа изобретений поясняется чертежами, где:

Фиг. 1 - персональный криптозащитный комплекс.

Фиг. 2 - схема устройства кассеты персонального криптозащитного комплекса.

Фиг. 3 - функциональная схема защитной оболочки.

Фиг. 4 - функциональная схема установления криптозащитного сеанса связи:

а) – обмен случайными числами Z и Z*;

б) – запись случайных чисел Z и Z* в ОЗУ;

в) – получение из чисел Z и Z* результирующего числа X;

г) – получение из числа X и чисел M n дочернего динамически преобразуемого кода;

д) – синхронное преобразование дочернего динамически преобразуемого кода в персональных криптозащитных комплексах обоих пользователей, шифрование, передача и дешифрование информации.

Фиг. 5 - функциональная схема передачи зашифрованного сообщения:

а) – пользователь А вводит в свой ПКК индивидуальный номер «I» ПКК адресата;

б) – получение из чисел Z и I результирующего числа X;

в) – пользователь А шифрует и отправляет электронное письмо вместе с числом Z;

г) – адресат вводит в свой ПКК полученное число Z и получает с помощью своего номера I результирующее число X;

д) – адресат вводит зашифрованное электронное письмо и получает его исходный текст.

Фиг. 6 - функциональная схема формирования электронного документа с паролем дешифрования:

а) – формирование электронного документа с паролем дешифрования;

б) – ввод команды на дешифрование электронного документа;

в) – дешифрование служебной информации электронного документа и сравнение паролей дешифрования;

г) – дешифрование электронного документа и вывод исходного текста пользователю;

Фиг. 7 - функциональная схема формирования электронного документа с наличием служебной информации и защиты от навязывания ложной информации:

а) – формирование электронного документа со служебной информацией;

б) – при дешифровании электронного документа служебная информация распознаётся при помощи служебных символов и выдаётся пользователю вместе со служебными символами;

в) – фальсификация электронного документа путём включения в текст служебной информации и служебных символов перед шифрованием;

г) – при дешифровании электронного документа с фальсифицированной служебной информацией служебные символы распознаются и удаляются из текста;

Фиг. 8 - функциональная схема формирования электронного документа с электронной цифровой подписью пользователя ПКК:

а) – в ответ на команду пользователя на подписание электронного документа ПКК выдаёт запрос на идентификацию пользователя;

б) – после введения идентификационных данных пользователя вводится электронный документ, к которому перед шифрованием автоматически добавляются электронная подпись пользователя, время и дата подписания, и индивидуальный номер ПКК пользователя;

в) – после дешифрования электронного документа, пользователю выводится электронная подпись, включающая дату и время подписания и индивидуальный номер ПКК пользователя, со служебными символами, позволяющими удостоверится в подлинности электронной подписи данного электронного документа.

Фиг. 9 - функциональная схема трёхэтапной передачи электронного документа с защитой от копирования:

а) – производится передача электронного документа с одного ПКК в другой, при этом электронный документ блокируется в обоих ПКК на определённый период времени Т1;

б) – в ответ на приём электронного документа отправляется пароль подтверждения загрузки электронного документа, при этом время блокировки электронного документа в обоих ПКК изменяется на Т2;

в) – в ответ на полученный пароль подтверждения загрузки электронного документа отправляется пароль подтверждения передачи электронного документа, при этом в ПКК отправителя заблокированный электронный документ удаляется из памяти, а в ПКК получателя электронный документ разблокируется;

Фиг. 10 - функциональная схема защиты от копирования компьютерной программы:

а) – производится передача пароля дешифрования с одного ПКК в другой, при этом пароль дешифрования блокируется в обоих ПКК на определённый период времени Т1;

б) – в ответ на приём пароля дешифрования отправляется пароль подтверждения загрузки пароля дешифрования, при этом время блокировки пароля дешифрования в обоих ПКК изменяется на Т2

в) – в ответ на полученный пароль подтверждения загрузки пароля дешифрования отправляется пароль подтверждения передачи пароля дешифрования, при этом в ПКК отправителя заблокированный пароль дешифрования удаляется из памяти, а в ПКК получателя пароль дешифрования разблокируется;

г) – с помощью разблокированного пароля дешифрования производится обработка компьютерной программы.

Фиг. 11 - функциональная схема передачи пароля дешифрования компьютерной программы на независимом носителе:

а) – в ПКК вводится команда и информация для записи пароля на независимый носитель с целью последующей передачи на другой ПКК;

б) – пароль в зашифрованном виде переносится на независимый носитель и автоматически удаляется из памяти ПКК;

в) – зашифрованный пароль отправляется в ПКК получателя, где производится сверка с текущей датой и индивидуальным номером ПКК, и в случае положительного результата дешифрованный пароль записывается в ППЗУ, но без права передачи до истечения даты, указанной в служебной информации;

г) – после истечения даты, указанной в служебной информации, пароль дешифрования может быть передан другому пользователю по той же схеме.

Фиг. 12 - функциональная схема одновременного обмена электронными документами, защищенными от копирования:

а) – перед обменом электронными документами, защищёнными от копирования, один из пользователей вводит команду об одновременном обмене электронными документами, затем производится передача электронных документов с одного ПКК в другой, при этом электронные документы блокируются в обоих ПКК на определённый период времени T1;

б) – в ответ на приём электронного документа отправляется пароль подтверждения загрузки электронного документа, при этом время блокировки электронного документа в обоих ПКК изменяется на T2, кроме того, пользователи имеют возможность просмотреть текст заблокированных электронных документов;

в) – пользователь вводит команду, подтверждающую передачу электронного документа, после чего в ПКК другого пользователя отправляется подтверждающий сигнал;

г) – после обмена подтверждающими сигналами производится синхронизация по последнему сигналу и одновременный обмен паролями подтверждения передачи электронного документа, при этом в ПКК отправителя заблокированный электронный документ удаляется из памяти, а в ПКК получателя электронный документ разблокируется.

Фиг. 13 - функциональная схема защиты от прослушивания информации в открытых линиях связи:

а) Схема противодействия пассивному прослушиванию:

Для формирования одноразового ключа сеанса связи пользователь A и сторонний пользователь должны обменяться случайными числами Z и Z*. Подслушивающий пользователь не может расшифровать перехваченную информацию, т.к. его кассета не сможет выработать такой же одноразовый ключ сеанса связи из перехваченных чисел Z и Z* , потому что для этого невозможно выполнить следующее условие : одно из чисел Z или Z* должно быть получено собственным генератором случайных чисел в кассете пользователя.

б) Схема противодействия активному прослушиванию:

Для формирования одноразового ключа сеанса связи пользователь A и сторонний пользователь должны обменяться случайными числами Z и Z*. В этой схеме для подслушивания информации между пользователями подслушивающий пользователь использует две кассеты для установления мнимого криптозащитного сеанса связи с помощью двух одноразовых ключей ZA и Z*B и получения дешифрованной информации на отрезке между своими кассетами. Для

противодействия данному прослушивания есть два простых способа обнаружения активного прослушивания :

1) после обмена случайными числами в кассетах пользователей формируются пароли подтверждения установления защищённого сеанса связи, причём для удобства эти пароли могут выражаться в словесной форме. Для того чтобы убедиться в отсутствии активного прослушивания, пользователям достаточно сообщить друг другу эти пароли, и в случае их полного совпадения гарантировано отсутствие прослушивания информации на линии связи;

2) обмен электронными визитками пользователей. Пользователь А сможет получить электронную визитку стороннего пользователя и соответственно наоборот только при отсутствии активного прослушивания.

в) Схема противодействия дешифрованию электронного письма:

Для формирования одноразового ключа шифрования электронного письма пользователь А использует индивидуальный номер кассеты стороннего пользователя и случайное число, которое отправляет вместе с зашифрованным электронным письмом. Подслушивающий пользователь не может расшифровать информацию в зашифрованном электронном письме, т.к. его кассета не сможет выработать такой же одноразовый ключ дешифрования из перехваченных чисел Z и I, потому что для этого невозможно выполнить следующее условие: число I должно являться индивидуальным номером кассеты пользователя.

Фиг.14 - функциональная схема передачи электронного письма с уведомлением:

а) – формирование, отправление и получение электронного письма с уведомлением в процессе криптозащитного сеанса связи;

б) – получатель электронного письма с уведомлением формирует уведомление и отправляет соответствующий сигнал отправителю;

в) – пользователи одновременно обмениваются между собой паролем дешифрования электронного письма на уведомление о получении данного письма.

Предпочтительный вариант осуществления изобретения

Персональный криптозащитный комплекс, выполненный в соответствии с изобретением, работает следующим образом. Пользователь подключает кассету 1 (фиг.1) к терминалу 2 и активизирует её путём подачи сигнала о начале работы. Активизированная кассета выдаёт пользователю запрос на право доступа пользователя. Пользователь вводит посредством терминального устройства 2 свои идентификационные данные, которые кассета сверяет с данными, ранее введёнными пользователем и сохранёнными в ППЗУ 13 (фиг.2). В случае совпадения данных кассета продолжает работу. Для того чтобы в процессе дальнейшей работы, при совершении криптозащитных операций, упростить и ускорить процедуру идентификации пользователя, пользователь подключает к терминалу с помощью поводка 8 идентификационный браслет 6, надетый на руку пользователя, при помощи защёлок 7 с датчиками фиксации. После первой успешной идентификации пользователя кассета проверяет

наличие подключённого идентификационного браслета и при обнаружении его генерирует несколько одноразовых случайных паролей, которые одновременно сохраняет в ППЗУ 13 кассеты и в ППЗУ идентификационного браслета 6. Перед каждой операцией, требующей проверки права доступа пользователя, кассета запрашивает у идентификационного браслета один из одноразовых паролей, получает пароль, сверяет его с паролями, сохранёнными в ППЗУ 13, и при совпадении паролей считает проверку доступа успешной. При этом использованный одноразовый пароль, удаляется из памяти кассеты и идентификационного браслета. При снятии браслета с руки датчики 7 фиксации защёлок подают сигнал в микропроцессор идентификационного браслета, после чего производится автоматическое удаление из памяти браслета всех неиспользованных одноразовых паролей. Дополнительно, для удобства пользователя, идентификационный браслет 6 и терминальное устройство 2 могут быть снабжены беспроводным интерфейсом для сопряжения с каналом беспроводной передачи данных. Если идентификационный браслет содержит аккумулятор, то его замена может производиться при подключении поводка 8 к терминалу 2 с помощью устройства автоматической замены аккумуляторов 9. Идентификационный браслет может также использоваться пользователем для доступа к объектам, снабжённым специальными электронными замками в которых сохраняют одноразовые пароли доступа. Причём одноразовые пароли доступа могут быть получены генераторами псевдослучайных чисел, находящимися в персональном криптозащитном комплексе пользователя и в электронном замке объекта доступа, работающими по аналогичной программе и вырабатывающими одинаковые одноразовые пароли доступа.

Так как производимые кассетой операции требуют усилённой защиты, то кассеты снабжена микропроцессором 16, выполненным с возможностью подавления и маскирования собственных микроизлучений и создания ложных микроизлучений. Микропроцессор 16 содержит дополнительные параллельные дорожки для подачи сигналов, компенсирующих микроизлучения собственных сигналов микропроцессора, и генератор для формирования ложных микроизлучений в диапазоне частот собственных микроизлучений микропроцессора. Кроме того, кассета 1 упакована в защитную оболочку 10, которая предотвращает изъятие информации из памяти 14 кассеты. В память 14 типа CMOS, записывается материнский код 15, на основе которого производится шифрование и дешифрование всей информации. Повреждение защитной оболочки 10 приводит к уничтожению материнского кода 15. Данная защита действует следующим образом. Аккумуляторная батарея 11 подаёт энергетические импульсы 31 (фиг.3) на светодиод 29, дозировка и периодичность которых контролируется программой блок контроля целостности защитной оболочки 23. Светодиод 29 генерирует кванты световой энергии 32, которые, отражаясь от светоотражающих поверхностей 26 и 27 распространяются через прозрачный слой 28 вокруг кассеты внутри защитной оболочки. Фотоэлементы 30, расположенные в различных местах на светоотражающей поверхности 27, поглощают кванты

световой энергии 32 и преобразуют их в энергоинформационные импульсы, которые измеряются и сравниваются с эталонными значениями с помощью программы блока 23 контроля целостности защитной оболочки. Если хотя бы одна из светоотражающих поверхностей будет повреждена, то значения энергоинформационных импульсов значительно изменятся. Такое изменение будет расценено программой блока контроля целостности защитной оболочки как разрушение защитной оболочки, и программа даст команду удалить из памяти 14 материнский код 15. При этом остальная информация сохранится в памяти кассеты.

Основной операцией, производимой кассетой персонального криптозащитного комплекса, является операция шифрования/дешифрования информации. Данная операция производится по алгоритму, заложенному в программе шифрования/дешифрования 21, записанной в ПЗУ 17. Ключами, на основании которых производится шифрование/ дешифрование, являются материнский код 15 состоящий из множества случайных чисел (M1, M2,..., MN), и временный ключ, состоящий по меньшей мере из одного случайного числа Z, вырабатываемого встроенным генератором 20 случайных чисел. Шифрование и дешифрование с использованием персональных криптозащитных комплексов, включает следующие этапы, осуществляемые в каждом из персональных криптозащитных комплексов:

1) подключение по меньшей мере двумя пользователями своих персональных криптозащитных комплексов 34 и 35 (фиг.4) к линии связи и установление ими количества участников криптозащитного сеанса связи,

2) выработка случайного числа Z 36 в персональном криптозащитном комплексе 34, и случайного числа Z* 37 в персональном криптозащитном комплексе 35 и сохранение данных чисел в оперативной памяти 18,

3) обмен по линии связи данными выработанных случайных чисел Z и Z* между упомянутыми персональными криптозащитными комплексами с установлением момента времени запуска формирования одноразового ключа сеанса связи,

4) синхронное формирование одноразового ключа сеанса связи X 38 путём считывания из оперативной памяти сохраненного случайного числа Z 36, выполнения заранее определённой арифметической операции над случайным числом Z 36, считанным из оперативной памяти, и случайным числом Z* 37, полученным от другого пользовательского криптозащитного устройства, для получения результирующего числа X и сохранение результирующего числа X в оперативной памяти 18 обоих устройств,

5) синхронное формирование динамически преобразуемого дочернего кода в персональных криптозащитных комплексах на основе материнского кода и одноразового ключа сеанса связи,

6) ввод и разделение исходной передаваемой информации 40 на пакеты определенного размера и шифрование пакетов с использованием динамически преобразуемого дочернего кода,

7) передача зашифрованных пакетов информации 41 по меньшей мере в один другой персональный криптозащитный комплекс,

8) прием зашифрованных пакетов информации 41 в упомянутом по меньшей мере одном другом персональном криптозащитном комплексе,

9) дешифрование принятых зашифрованных пакетов с использованием динамически преобразуемого дочернего кода,

10) объединение дешифрованных пакетов в исходную информацию и вывод информации 42 пользователю,

при этом повторяют этапы (5)-(10) для передачи информации в обратном направлении в том же сеансе связи.

Момент времени запуска формирования одноразового ключа сеанса связи X 38 устанавливают по моменту передачи и приема данных, соответствующих последнему из обмениваемых по линии связи на этапе (3) упомянутых случайных чисел.

Преобразование динамического дочернего кода 39 синхронизируют по моменту передачи и приема каждого из пакетов информации.

Одновременно с формированием дочернего сеанса связи в каждом из персональных криптозащитных комплексах формируют одноразовый пароль подтверждения установления защищённого сеанса связи, который совпадает у данных участников сеанса связи и с помощью которого удостоверяются в установлении защищённого сеанса связи (фиг. 13,б). При осуществлении дуплексной связи с использованием персональных криптозащитных комплексов 34 и 35 в каждом из них синхронно формируют два динамически преобразуемых дочерних кода на основе материнского кода и одноразового ключа сеанса связи. Если для одного из персональных криптозащитных комплексов первый динамически преобразуемый дочерний код используется для шифрования информации, то для другого персонального криптозащитного комплекса упомянутый динамически преобразуемый дочерний код используется для дешифрования информации и соответственно считается вторым динамически преобразуемым дочерним кодом. При этом преобразование первого динамически преобразуемого дочернего кода на этапах (6) и (9) синхронизируют по моменту передачи каждого из пакетов информации, а для второго динамически преобразуемого дочернего кода преобразование на этапах (6) и (9) синхронизируют по моменту приёма каждого из пакетов информации, таким образом, синхронизация каждой пары динамически преобразуемых дочерних кодов осуществляется независимо от другой пары.

В случае, когда шифрование информации производится в режиме электронного письма, для дальнейшего отправления зашифрованной информации пользователю-адресату, отправитель вводит в кассету 1 посредством терминального устройства 2 индивидуальный номер 19 персонального криптозащитного комплекса адресата (фиг. 5) и вводит команду на

шифрование сообщения 40. Шифрование и дешифрование сообщения включает следующие этапы:

- в персональном криптозащитном комплексе 34 (фиг.5), являющемся отправителем информации 40, вырабатывают случайное число Z 36 и сохраняют его в оперативной памяти 18, вводят индивидуальный номер I - 19 персонального криптозащитного комплекса 35 получателя информации, формируют одноразовый ключ шифрования путем считывания из оперативной памяти сохраненного случайного числа Z и индивидуального номера I, выполняют арифметическую операцию над случайным числом Z и индивидуальным номером I для получения результирующего числа X 38 и сохраняют результирующее число X в оперативной памяти 18, формируют динамически преобразуемый дочерний код 39 на основе материнского кода 15 и одноразового ключа шифрования 38, вводят и разделяют отправляемую информацию 40 на пакеты определенного размера, шифруют пакеты с использованием динамически преобразуемого дочернего кода и выводят зашифрованные пакеты информации 43 для записи на носитель совместно со случайным числом Z 36 для дальнейшей передачи получателю, при этом преобразование динамического дочернего кода производится по моменту окончания шифрования заранее определенного количества байтов информации;

- в персональном криптозащитном комплексе 35, являющемся получателем информации, считывают из ПЗУ 17 индивидуальный номер I- 19 персонального криптозащитного комплекса получателя информации и сохраняют его в оперативной памяти 18, вводят в оперативную память число Z 36, полученное от отправителя информации, формируют одноразовый ключ шифрования путем считывания из оперативной памяти сохраненного случайного числа Z и индивидуального номера I, выполняют арифметическую операцию над случайным числом Z и индивидуальным номером I для получения результирующего случайного числа X 38 и сохраняют результирующее случайное число X в оперативной памяти, формируют динамически преобразуемый дочерний код 39 на основе материнского кода 15 и одноразового ключа шифрования 38, вводят зашифрованные пакеты информации 43 с носителя и дешифруют пакеты с помощью динамического дочернего кода 39, при этом преобразование динамического дочернего кода производится по моменту окончания дешифрования заранее определенного количества байтов информации, и объединяют пакеты и выводят дешифрованную информацию 44 получателю информации.

Оба способа шифрования/дешифрования информации с использованием персональных криптозащитных комплексов предотвращают дешифрование перехваченной информации подслушивающим пользователем 81 (фиг.13). Основным препятствием для дешифрования информации пользователем 81, использующем аналогичные устройства, что и пользователи 34 и 35, является то, что программа обработки информации 22, записанная в ПЗУ 17 каждой кассеты, контролирует все команды пользователя, и в случае, если команды пользователя некорректны с точки зрения программы, такие команды игнорируются. Так кассета

пользователя 81 не сможет сформировать одноразовый ключ сеанса связи 38 из перехваченных чисел 36, 37 в а) (фиг.13) и 36, 19 в в) (фиг. 13), так как не выполнены следующие условия: в (а) одно из случайных чисел 36 или 37 обязательно должно быть получено собственным генератором случайных чисел, в (в) число 19 должно быть собственным индивидуальным номером кассеты. В случае с вариантом (б) (фиг. 13) одновременно с формированием дочернего ключа сеанса связи в каждом из персональных криптозащитных комплексов 34 и 35 формируют одноразовый пароль подтверждения установления защищённого сеанса связи, который совпадает у данных участников сеанса связи только при отсутствии активного прослушивания и с помощью которого удостоверяются в установлении защищённого сеанса связи.

При шифровании электронных документов часто возникает необходимость в том, чтобы с текстом электронного документа могли в дальнейшем ознакомиться и другие пользователи персональных криптозащитных комплексов. Для этого имеется режим шифрования с применением пароля дешифрования данного электронного документа 45 (фиг.6). При включении этого режима по команде 46 пользователя на установление пароля в кассете 1 перед началом шифрования генерируется случайное число Y 48, являющееся в дальнейшем паролем дешифрования электронного документа. Число Y вставляется программой обработки информации в начало шифруемого электронного документа, причём данное число с обеих сторон выделяется служебными символами 47, которые вместе с числом Y 48 образуют служебную информацию. Пользователю выводят число Y, которое пользователь передаёт другим пользователям вместе с зашифрованным электронным документом.

Дешифрование электронного документа происходит следующим образом. Пользователь 35 вводит в кассету команду 50 на дешифрование электронного документа и вводит пароль дешифрования – число Y, затем вводит начальную часть зашифрованного электронного документа, содержащую зашифрованное число Y. В кассете на основании введённых данных формируется одноразовый ключ X, и с его помощью формируется дочерний динамически преобразуемый код, с помощью которого производится дешифрование той части электронного документа, которая содержит число Y. Затем производится сравнение введённого пользователем числа Y и расшифрованного числа Y. Если числа совпадут, то кассета продолжает дешифрование электронного документа и выводит расшифрованный текст электронного документа пользователю. Сравнение чисел Y может происходить и другим способом, а именно: шифруется вводимое число Y, его криптограмма сверяется с зашифрованным числом Y, и в случае совпадения кассета начинает дешифрование электронного документа. Для удобства пользователя, шифрующего электронный документ с применением пароля дешифрования, пользователь может использовать в качестве пароля собственный набор символов D, который вводит в кассету вместе с командой на установление пароля дешифрования. Затем с помощью генератора случайных чисел в кассете вырабатывают

случайное число Y и совершают определённую обратимую арифметическую операцию между упомянутым случайным числом Y и числом D, получая в итоге число F, которое выводят пользователю вместе с зашифрованным электронным документом для передачи персональным криптозащитным комплексам других пользователей или для записи на носители. По меньшей мере в одном любом персональном криптозащитном комплексе, вводят число F, вводят пароль дешифрования D, совершают между данными числами определённую арифметическую операцию, сохраняют полученный результат Y в оперативной памяти персонального криптозащитного комплекса и используют его для дешифрования вводимой информации. Кроме того, в служебной информации зашифрованного электронного документа, могут содержаться команды, включённые по команде пользователя персональным криптозащитным комплексом 34, адресованные персональным криптозащитным комплексам и устанавливающие дату и время дешифрования электронного документа, только по истечении которых персональный криптозащитный комплекс любого пользователя, дешифрующего электронный документ, произведёт его дешифрование, а также могут быть включены заранее определённые команды, позволяющие вносить определённые изменения в содержание электронного документа.

Программа шифрования/дешифрования должна обеспечивать противодействие к вычислению материнского кода путём сопоставления неограниченного массива исходной информации и такого же массива криптограммы данной информации. Для этого в программу включены операции, имеющие необратимый характер. Шифрование и дешифрование протекает следующим образом:

1) считывают из оперативной памяти 18 число X 38, считывают из памяти 14 первое число M1 материнского кода 15, выполняют арифметическую операцию над считанными числами X и M1 для получения первого результирующего числа определённой разрядности, которое сохраняют в оперативной памяти 18, причём отделяют от данного числа k – младших разрядов и присваивают полученному числу P1 номер, соответствующий отделённому числу k-ной разрядности,

2) считывают из оперативной памяти 18 упомянутое первое число P1, считывают из памяти второе число M2 материнского кода 15, выполняют арифметическую операцию над считанными числами P1 и M2 для получения второго числа P2 и сохраняют упомянутое число P2 в оперативной памяти 18,

3) повторяют этап (2) для чисел P(i-1) и Mi, где i = 3,...,N, для получения множества чисел P3...PN, сохраненных в оперативной памяти 18,

4) формируют из множества чисел P1...PN два подмножества, первое из которых состоит из чисел, соответствующих k младшим разрядам чисел P1...PN, а второе – из чисел, соответствующих m старшим разрядам чисел P1...PN, группируют второе подмножество чисел

в таблицу по адресам, соответствующим числам первого подмножества, количество которых равно возможному количеству чисел первого подмножества,

5) выбирают столбец таблицы с максимальным количеством чисел из второго подмножества или все столбцы с одинаковым максимальным количеством чисел и производят последовательно арифметическую операцию с последовательными парами чисел выбранных столбцов, в результате чего получают промежуточное число К,

6) повторяют для числа К и множества чисел P1...PN этапы обработки (1) – (4), причем на этапе (4) выбирают k=8 бит и полученные числа второго подмножества распределяют в таблицу с 256 столбцами, пронумерованными одним из 256 байтов, причем столбцы с количеством чисел менее двух дополняют числами из столбцов с максимальным количеством чисел,

7) производят последовательно арифметическую операцию с последовательными парами чисел столбцов, для получения для каждого столбца числа Q1... Q256 определенной разрядности,

8) формируют из множества чисел Q1...Q256 два подмножества, первое из которых состоит из чисел, соответствующих 4 младшим разрядам чисел Q1...Q256, а второе – из чисел, соответствующих остальным старшим разрядам чисел Q1...Q256, группируют второе подмножество чисел в таблицу размером 100 x 100 по адресам, соответствующим числам первого подмножества,

9) формируют таблицу размером 16 x 16 из байтов, соответствующих второму подмножеству чисел пункта (8), путем последовательного построчного прохождения таблицы размером 100 x 100, нахождения в ней ячеек с числами упомянутого второго подмножества и записи в той же последовательности в таблицу размером 16 x 16 байтов, соответствующих найденным числам,

10) производят арифметические операции над числами второго подмножества этапа (8), соответствующими по меньшей мере двум соседним байтам для каждого байта из таблицы размером 16 x 16, для получения двух новых подмножеств и второй таблицы размером 16 x 16, повторяя этапы (8) – (9);

этапы (1)–(10) осуществляют одинаково как при шифровании, так и при дешифровании; далее шифрование информации производят путем представления информации в 8-битных байтах, подстановки их в первую таблицу, сопоставления координат байтов исходной информации в первой таблице с аналогичными координатами байтов во второй таблице и замены байтов исходной информации на байты из второй таблицы с упомянутыми координатами и выводят полученные в результате замены байты криптограммы для последующей передачи, а дешифрование информации производят путем замены полученных байтов криптограммы на байты исходной информации путем подстановки их во вторую таблицу, сопоставления координат байтов криптограммы во второй таблице с аналогичными

координатами байтов в первой таблице и замены байтов криптограммы на байты из первой таблицы с упомянутыми координатами и выводят полученные в результате замены байты пользователю;

11) после шифрования и дешифрования определенного количества байтов информации с помощью сформированного дочернего кода обновляют первую и вторую таблицы размером 16 x 16 путем удаления первой таблицы, замены ее второй таблицей и формированием новой второй таблицы согласно пункту (10).

Арифметические операции с числами могут производить путем деления одного числа на другое и сохранения полученного результата в оперативной памяти 18, затем в полученном числе выделяют n значащих цифр, которые представляют в виде целого натурального числа разрядности n и сохраняют это число вместо результата деления в памяти для дальнейшего использования.

Для ускорения процессов шифрования и дешифрования используется следующий способ: перед началом шифрования и дешифрования информации в каждом персональном криптозащитном комплексе создают несколько таблиц 16 x 16, повторяя этапы (8) – (9), общим количеством R, заранее определённым и большим двух, и сохраняют их в оперативной памяти 18, а шифрование и дешифрование пакета информации, состоящего из определенного количества байтов, производят с помощью двух таблиц 16 x 16, начиная с первой и второй таблиц, затем следующий пакет информации шифруют и дешифруют с помощью первой и третьей таблиц и так далее до последней таблицы 16 x 16, которую также используют в паре с первой таблицей, после чего удаляют первую таблицу, заменяют ее второй таблицей, вторую таблицу заменяют третьей таблицей и так далее до последней таблицы, которую ставят на место предпоследней таблицы, а на место последней таблицы ставят новую таблицу 16 x 16, сформированную согласно пункту (10), и продолжают шифрование и дешифрование пакетов информации, начиная с первой и второй таблиц.

Для усиления криптостойкости можно заменить 8-битное представление информации на 9-битное. В этом случае повторяют этапы обработки (1) – (4), причем на этапе (4) выбирают k = 9 бит и полученные числа второго подмножества распределяют в таблицу с 512 столбцами, пронумерованными одним из 512 байтов, причем столбцы с количеством чисел менее двух дополняют числами из столбцов с максимальным количеством чисел, таблицу 16 x 16 заменяют таблицей 8 x 8 x 8, а таблицу 100 x 100 заменяют таблицей 100 x 100 x 100.

При шифровании и дешифровании электронных документов вводят зависимость преобразования таблиц от шифруемой/дешифруемой информации на этапе (11), что даёт защиту от внесения изменений в зашифрованный текст электронного документа, так как один изменённый символ криптограммы приведёт к распространению изменений на весь последующий текст при дешифровании электронного документа.

Для дополнительной защиты от внесения изменений в зашифрованную информацию применяют хеширование каждого пакета исходной информации с добавлением к пакету результата хеширования, шифруют полученный пакет и хешируют второй хеш-функцией с добавлением результата второго хеширования. Устанавливают подлинность зишифрованной информации следующим образом: принимают переданные зашифрованных пакеты и второй результат хеширования, добавленный к каждому пакету, восстанавливают частично потерянные или искаженные при передаче данные с использованием второго результата хеширования путем обратного хеширования с получением по меньшей мере одного варианта зашифрованного пакета информации, дешифруют по меньшей мере один вариант зашифрованного пакета информации и записывают в оперативную память по меньшей мере один вариант дешифрованного пакета. Производят обратное хеширование дешифрованных пакетов информации с использованием первого результата хеширования и проводят поиск подлинного варианта пакета исходной информации, причем только при нахождении упомянутого подлинного варианта он выводится пользователю, а все остальные ложные варианты дешифрованного пакета удаляются из оперативной памяти.

Задачу аутентификации электронных документов 45 (фиг.8) решают следующим образом:

Вводят в кассету 1 персонального криптозащитного комплекса посредством терминального устройства 2 команду 57 на подписание электронного документа 45. Кассета выводит пользователю запрос 58 на идентификацию пользователя, пользователь вводит свои идентификационные данные 59. При соответствии введённых идентификационных данных с сохранёнными данными кассета начинает шифрование электронного документа 45 в режиме защиты от внесения изменений. Текст электронного документа вводится через терминальное устройство 2 с устройства ввода либо с носителя. После завершения шифрования текста, к тексту электронного документа под контролем программы обработки информации добавляется первый служебный символ 47, служебная информация 54 и замыкающий ее второй служебный символ 47. При этом шифрование текста электронного документа, служебной информации и служебных символов производится как шифрование единого документа одним одноразовым ключом X 38. Служебная информация 54 в данном случае состоит из данных пользователя 24, представляющих электронную цифровую подпись, индивидуального номера персонального криптозащитного комплекса 19, даты и времени подписания, взятые от встроенных часов 12. При дешифровании электронного документа 53 сторонними пользователями 35, сначала дешифруется текст электронного документа и выводится пользователю через терминальное устройство 2, а затем дешифруется служебная информация 54, определяемая программой обработки информации 22 с помощью служебных символов 47, и выводится пользователю на дисплей с указанием на то, что данная информация действительно является электронной цифровой подписью и именно данного электронного документа. Устанавливают с помощью

электронной цифровой подписи дату и время подписания и лицо, подписавшее электронный документ, так как данные пользователя в электронной цифровой подписи предварительно заносятся регистратором в ПЗУ 17 персонального криптозащитного комплекса одновременно с их регистрацией в общедоступной базе данных 85 (фиг.13). Кроме того, электронная цифровая подпись включает в себя электронную фотографию пользователя, которая позволяет идентифицировать электронную цифровую подпись без обращения к базе данных.

Регистрация электронной цифровой подписи пользователя персонального криптозащитного комплекса производится следующим образом:

- берут данные пользователя 24, индивидуальный номер 19 кассеты 1 его персонального криптозащитного комплекса 34, заявление пользователя записанное цифровой видеокамерой и содержащее информацию, позволяющую идентифицировать пользователя,

- вводят информацию в персональный криптозащитный комплекс регистратора, подписывают полученную информацию электронной цифровой подписью регистратора, производят её шифрование и отправляют на центральный сервер,

- вводят информацию в центральный криптозащитный комплекс, производят дешифрование полученной информации, заносят дешифрованную информацию в базу данных 85 электронных цифровых подписей, формируют из полученной информации электронную цифровую подпись пользователя, заверяют её электронной цифровой подписью центрального криптозащитного комплекса содержащей заранее определённую информацию, шифруют и отправляют в персональный криптозащитный комплекс 34 пользователя,

- принимают и дешифруют информацию, в соответствии с заложенной программой проверяют электронную цифровую подпись пользователя на соответствие типовому шаблону, проверяют наличие электронной цифровой подписи центрального криптозащитного комплекса, сверяют индивидуальный номер, содержащийся в полученной электронной цифровой подписи пользователя, с индивидуальным номером персонального криптозащитного номера пользователя и в случае положительных результатов записывают электронную цифровую подпись пользователя в ПЗУ 17 кассеты его персонального криптозащитного комплекса.

В отличие от электронной цифровой подписи, хранимой в ПЗУ 17 кассеты 1 пользователя, электронная печать содержит данные определённого юридического лица и хранится в ППЗУ 13 кассеты 1. Электронная печать, в отличие от электронной подписи, может передаваться с одной кассеты в другую с одновременным удалением из ППЗУ 13 кассеты, с которой производится передача. Регистрация электронной печати производится аналогично регистрации электронной подписи.

Персональный криптозащитный комплекс позволяет придать любому электронному документу возможность удостоверять с его помощью права собственности любым пользователем, владеющим данным электронным документом без внесения изменений в содержание электронного документа. Частным случаем такого электронного документа:

является электронный вексель на предъявителя. Данный электронный документ обладает свойством защиты от копирования по аналогии с документами на бумажном носителе, защищаемыми от копирования различными способами (голографические и водяные знаки, фоновый рисунок и вшитые нити). Специфика защиты электронного документа от копирования состоит в том, что от копирования защищается не открытый текст электронного документа, а его криптограмма либо пароль дешифрования криптограммы электронного документа. Соответственно, доказательством владения электронным документом, защищённым от копирования, является возможность пользователя персональным криптозащитным комплексом получить дешифрованный текст данного электронного документа с помощью кассеты, в которой хранится криптограмма либо пароль дешифрования криптограммы электронного документа. А открытый текст электронного документа, защищённого от копирования, считается его копией. Персональный криптозащитный комплекс позволяет придать любому электронному документу свойство защиты от копирования. Для этого при введении пользовательской информации в персональный криптозащитный комплекс 34 (фиг.9) вводят команды пользователя для установки режима обработки пользовательской информации, формирования некопируемого электронного документа и обрабатывают введенную пользовательскую информацию.

Затем формируют с помощью программы обработки информации 22 в соответствии с установленным режимом обработки пользовательской информации и ранее полученной информации служебную информацию 54, объединяют ее с обработанной пользовательской информацией, получая электронный документ 60, причем атрибуты электронного документа в виде служебной информации 54 выделяют от обработанной пользовательской информации предварительно определенными служебными символами 47, и в соответствии с командой пользователя - сформировать некопируемый электронный документ, - включают в служебную информацию определённую команду для персональных криптозащитных комплексов в виде типового набора символов, заранее введённых в ПЗУ 17 в составе программы обработки информации 22 и сохраняют полученный электронный документ 60 в отделе ППЗУ 13, предназначенном для некопируемых электронных документов, персонального криптозащитного комплекса.

Передача электронного документа с защитой от копирования путём защиты от копирования криптограммы электронного документа осуществляется следующим способом:

- устанавливают защищённый сеанс связи с применением персональных криптозащитных комплексов 34 и 35 на основе одноразового ключа сеанса связи 38, сформированного с использованием случайных чисел и вводят команду пользователя передать записанный в ППЗУ 13 не копируемый электронный документ 60 другому абоненту установленного сеанса связи,

- шифруют динамически преобразуемым дочерним кодом 39 электронный документ 60, считывая при этом из служебной информации 54 команду о некопируемости электронного документа, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в другой персональный криптозащитный комплекс 35,

- в соответствии с командой о некопируемости по окончанию передачи некопируемого электронного документа производят его блокирование 61 на заранее определённый период времени T1 в ППЗУ 13,

- принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

- осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов 47, находят с помощью служебных символов служебную информацию 54, содержащую команду о некопируемости электронного документа, записывают электронный документ в отдел ППЗУ 13, предназначенный для некопируемых электронных документов, и блокируют его 61 на заранее определённый период времени T1,

- в персональном криптозащитном комплексе 35 принимающей стороны формируют пароль подтверждения загрузки 62 электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс 34 отправляющей стороны,

- в случае неполучения отправителем от получателя пароля подтверждения загрузки 62 электронного документа в течение периода времени T1 производят разблокирование электронного документа в ППЗУ персонального криптозащитного комплекса 34 отправителя, а последующее получение упомянутого пароля игнорируется,

- в случае неотправления получателем отправителю пароля подтверждения загрузки 62 электронного документа в течение периода времени T1 производят удаление электронного документа из ППЗУ 13 персонального криптозащитного комплекса 35,

- принимают пароль подтверждения загрузки 62 электронного документа в персональном криптозащитном комплексе 34 отправляющей стороны, формируют пароль подтверждения передачи 63 электронного документа и запрашивают подтверждение пользователя на отправление данного пароля в персональный криптозащитный комплекс 35 принимающей стороны,

- в случае, если пользователь не даёт подтверждение на отправление пароля 63 в течение заранее определённого периода времени T2, то по истечению данного периода времени в ППЗУ 13 персонального криптозащитного комплекса 34 отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ 13 персонального криптозащитного комплекса 35 получателя упомянутый электронный документ автоматически удаляют,

- в случае, если пользователь даёт подтверждение на отправление пароля 63 в течение периода времени Т2, то данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс 35 получателя, при этом упомянутый электронный документ 61 автоматически удаляют из ППЗУ 13 персонального криптозащитного комплекса 34 отправителя, а в ППЗУ 13 персонального криптозащитного комплекса 35 получателя после получения им пароля подтверждения передачи 63 электронного документа 60 автоматически производят разблокирование упомянутого электронного документа, после чего вводят команды пользователя, устанавливают режим обработки дешифрованной информации в соответствии с командами пользователя, командами, полученными из служебной информации, ранее введённой информацией и программой обработки информации 22 и выводят обработанную информацию 60 пользователю вместе со служебными символами 47, которые устанавливают подлинность атрибутов полученного электронного документа.

В случае если электронный документ 60, защищённый от копирования, в частности электронный вексель, содержит переменный номинал, обозначенный предварительно определённым образом с помощью служебных символов 47, то после дешифрования данного электронного документа определяют в служебной информации 54 информацию о переменном номинале электронного документа и выводят данную информацию пользователю; дробят электронный документ 60 на произвольные части, изменяя с помощью программы обработки информации 22 номиналы частей таким образом, что их общая сумма, остаётся неизменной, при этом остальные характеристики и атрибуты частей электронного документа также остаются неизменяемыми; отправляют части электронного документа в другие персональные криптозащитные комплексы; принимают в персональный криптозащитный комплекс несколько одинаковых электронных документов 60 с переменным номиналом и автоматически с помощью программы обработки информации 22 собирают в единый электронный документ, суммируя их номиналы.

Если электронным документом 60 с переменным номиналом является электронный переводной банковский вексель с заранее определённым сроком погашения, содержащий в служебной информации 54 электронного документа данные банка, выдавшего вексель, включая электронные цифровые подписи банка, сформированные с помощью персонального криптозащитного комплекса, данные пользователя, которому выдан вексель, валюту и номинал векселя, а также дату погашения векселя, после которой в банке произведут разблокирование оставшейся на счету пользователя залоговой суммы денег, которые досрочно передадут любому предъявителю данного электронного векселя либо его части, после того как примут электронный вексель в персональный криптозащитный комплекс банка, идентифицируют данные электронного векселя, определят его номинал, и в случае, если указанная в электронном векселе дата погашения не превышает текущей даты, выдадут предъявителю сумму, соответствующую номиналу предъявленного электронного векселя.

Если электронным документом 60 с переменным номиналом являются электронные наличные деньги, то расчёты электронными наличными деньгами производятся следующим образом: подключают персональные криптозащитные комплексы 34 и 35 друг к другу напрямую либо с использованием канала связи; устанавливают защищённый сеанс связи с применением персональных криптозащитных комплексов на основе динамически преобразуемого динамического кода 39 сформированного с помощью одноразового ключа сеанса связи 38, полученного с использованием случайных чисел 36 и 37 и вводят команду пользователя передать записанный в ППЗУ 13 электронные наличные деньги определённой валюты и суммы другому абоненту установленного сеанса связи; проверяют наличие в ППЗУ 13 персонального криптозащитного комплекса 34 записи, соответствующей по форме и содержанию электронным наличным деньгам требуемой валюты; в случае наличия в ППЗУ 13 упомянутой записи считывают сумму, соответствующую электронным наличным деньгам и сверяют с запрашиваемой суммой; в случае, если запрашиваемая сумма не превышает считанную сумму, выводят пользователю запрос на его идентификацию; вводят в персональный криптозащитный комплекс информацию и сверяют ее с хранимыми в персональном криптозащитном комплексе данными 24, соответствующими идентифицирующими пользователя; в случае совпадения, с помощью заранее введённой программы обработки информации 22 формируют типовой электронный документ, содержащий запись электронных денег на запрашиваемую пользователем валюту и сумму; одновременно производят изменение записи электронных наличных денег, хранимых в ППЗУ 13 уменьшая их стоимость на передаваемую сумму; и шифруют динамически преобразуемым дочерним кодом 39 упомянутый электронный документ, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в персональный криптозащитный комплекс пользователя, с которым установлен защищённый сеанс связи; по окончанию успешной передачи электронного документа производят его удаление из ППЗУ 13; принимают электронный документ, производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации и производят запись в ППЗУ 13 соответствующей по форме и содержанию полученным электронным наличным деньгам.

В случае, когда для защиты от копирования используется пароль 64 (фиг.10) дешифрования криптограммы, формируют пароль дешифрования на основе случайного числа и записывают его в отдел ППЗУ 13, предназначенный для некопируемых паролей дешифрования и закрытый для пользователей, формируют динамически преобразуемый дочерний код 39 на основе материнского кода 15 и пароля дешифрования 64; вводят в персональный криптозащитный комплекс информацию, в том числе компьютерную программу, и производят её шифрование с использованием упомянутого пароля дешифрования, выводят зашифрованную информацию 66 пользователю для записи на

носитель или для передачи другому пользователю, вводят команду передать пароль дешифрования 64 другому пользователю в процессе защищённого сеанса связи, шифруют пароль дешифрования на основе одноразового ключа 38, сформированного с использованием по меньшей мере одного случайного числа и выводят его для передачи. Передачу пароля дешифрования 64 производят аналогично передаче электронных документов, защищённых от копирования.

Защищать от копирования в этом случае можно не только электронные документы, но также компьютерные программы и базы данных. В этом случае дешифрованный фрагмент 67 компьютерной программы 66 записывается в ОЗУ 18 кассеты. Обработка дешифрованных фрагментов программы ведётся параллельно на двух процессорах: микропроцессоре 16 кассеты и микропроцессоре 68 компьютера с частичным использованием ОЗУ 69 компьютера. Так как часть операций обрабатываемых фрагментов 70 производится не покидая кассеты 1, то полностью восстановить дешифрованные фрагменты зашифрованной программы 66 практически невозможно.

Если необходимо ограничить период действия пароля дешифрования по времени или количеству использования, делают следующее: включают в пароль дешифрования соответствующие служебные команды и выделяют их служебными символами 47; шифруют полученные служебные команды в составе пароля дешифрования 64 и выводят для дальнейшей записи на носитель или передачи другому пользователю, сохраняя при этом пароль дешифрования в ППЗУ 13, одновременно блокируют доступ к паролю дешифрования 64, оставшемуся в ППЗУ 13 персонального криптозащитного комплекса пользователя, на заранее определённый промежуток времени; вводят или соответственно принимают зашифрованный пароль дешифрования 64, с включёнными в него служебными командами; выделяют с помощью служебных символов 47 служебные команды и производят операции с данным паролем дешифрования 64 в соответствии с полученными командами из служебной информации 54, а именно: удаляют из памяти персонального криптозащитного комплекса пароль дешифрования 64 по истечении указанного в служебной информации времени или после использования пароля дешифрования указанное в служебной информации количество раз.

Для передачи пароля дешифрования 64 с одного персонального криптозащитного комплекса в другой можно воспользоваться независимым носителем 73 (фиг.11). В этом случае добавляют к паролю дешифрования 64 служебную информацию 54, выделенную служебными символами 47, с указанием индивидуального номера персонального криптозащитного комплекса 19 получателя, а также даты и времени, по истечении которых получатель данного пароля дешифрования сможет передать его другим пользователям криптозащитных персональных комплексов. Одновременно в персональном криптозащитном комплексе 34 отправителя пароля дешифрования формируют электронное письмо, в которое включают пароль дешифрования 64 с добавленной к нему служебной информацией 54, а также

дополнительно указывают дату и время в виде служебной информации, только до истечения которых персональный криптозащитный комплекс получателя электронного письма сможет расшифровать данное сообщение, причём, дату и время дешифрования электронного письма указывают меньшую или аналогичную дате и времени, указанных в служебной информации пароля дешифрования. Шифруют сформированное электронное письмо динамически преобразуемым кодом на основе одноразового ключа, формируемого из случайного числа и индивидуального номера персонального криптозащитного комплекса получателя данного электронного письма и добавляют к зашифрованному электронному письму упомянутое случайное. Выводят зашифрованное электронное письмо 72 и случайное число для передачи адресату вместе с зашифрованной с помощью пароля дешифрования информацией; записывают зашифрованное электронное письмо 72, содержащее пароль дешифрования 64, вместе со случайным числом на носитель 73 или передают по линии связи и по окончании передачи удаляют пароль дешифрования из ППЗУ 13 персонального криптозащитного комплекса 34 отправителя. Принимают зашифрованное электронное письмо 72, случайное число и зашифрованную информацию 66; вводят случайное число в ОЗУ 18 персонального криптозащитного комплекса 35 и считывают индивидуальный номер персонального криптозащитного комплекса 19 из ПЗУ 17, также записывая его в ОЗУ 18; формируют одноразовый ключ на основе введённого случайного числа и считанного индивидуального номера, формируют динамически преобразуемый код на основе одноразового ключа и вводят в персональный криптозащитный комплекс 35 зашифрованное электронное письмо 72, производят дешифрование электронного письма с помощью динамически преобразуемого кода и записывают в ОЗУ 18 дешифрованный текст электронного письма 72, определяют служебную информацию 54 с помощью служебных символов 47, находят служебную информацию с указанием окончательных даты и времени дешифрования электронного письма и сверяются с датой и временем во встроенных часах 12 и в случае превышения указанных даты и времени над текущими производят удаление данного электронного письма из ОЗУ 18, находят пароль дешифрования 64, включающий дату и время, по истечении которых может быть произведена передача пароля дешифрования другим пользователям, и записывают в отдел ППЗУ 13 персонального криптозащитного комплекса 35, предназначенный для не копируемых паролей дешифрования и закрытый для пользователей ППЗУ. Вводят в персональный криптозащитный комплекс информацию, в том числе компьютерную программу, и производят дешифрование на основе динамически преобразуемого кода, сформированного с помощью считанного из ППЗУ пароля дешифрования; по истечении даты и времени, указанных в служебной информации, включённой в пароль дешифрования, удаляют из ППЗУ 13 данную служебную информацию, одновременно снимая ограничение на дальнейшую передачу пароля дешифрования 64 другим пользователям.

Электронные документы с защитой от копирования (включая пароли дешифрования 64) могут передаваться другими способами, получаемыми варьированием периодов времени T1 и T2 и добавлением дополнительных данных в виде номеров N1 и N2.

Так, к электронному документу в служебную информацию добавляют временный индивидуальный номер N2, формируемый генератором случайных чисел 20, и вводят произвольное значение времени T2, которые шифруют вместе с электронным документом.

Вводят команду передать электронный документ другому пользователю в процессе защищённого сеанса связи или в зашифрованном электронном письме; по окончании передачи данного электронного документа производят его блокирование на заранее определённый период времени T1 в ППЗУ 13 отправителя и отмечают его присвоенным временным индивидуальным номером; в случае сбоев при передаче электронного документа отправитель осуществляет повторное отправление данного электронного документа с теми же сопутствующими данными; принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации; осуществляют поиск и выделение служебной информации 54 из дешифрованной информации с помощью служебных символов 47, находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа и временный индивидуальный номер данного документа; сверяют данный номер на наличие в ППЗУ 13 заблокированного электронного документа с таким же номером и в случае отсутствия совпадения записывают электронный документ в отдел ППЗУ 13, предназначенный для некопируемых электронных документов, отмечают его присвоенным временным индивидуальным номером и блокируют электронный документ на заранее определённый период времени T1. В персональном криптозащитном комплексе 35 принимающей стороны на основе случайного числа формируют пароль подтверждения загрузки 62 электронного документа, автоматически добавляют к нему упомянутый временный индивидуальный номер N2 данного электронного документа, записывают копию пароля в ППЗУ 13 и в зашифрованном виде передают пароль подтверждения загрузки 62 электронного документа в персональный криптозащитный комплекс 34 отправляющей стороны в процессе защищённого сеанса связи или в зашифрованном электронном письме; принимают пароль подтверждения загрузки 62 электронного документа в персональном криптозащитном комплексе 34 отправляющей стороны, находят в ППЗУ 13 заблокированный электронный документ, отмеченный номером, соответствующим номеру, полученному с паролем, и в случае наличия заблокированного электронного документа и совпадения номеров формируют пароль подтверждения передачи электронного документа 63 с использованием пароля подтверждения загрузки электронного документа, автоматически включая в него упомянутый временный индивидуальный номер N2 электронного документа; запрашивают подтверждение пользователя на отправление данного пароля в персональный

криптозащитный комплекс принимающей стороны. В случае, если пользователь не даёт подтверждение на отправление пароля 63 в течение произвольного периода времени T2, значение которого заранее вводится отправителем при установлении режима отправления электронного документа, то по истечении данного периода времени в ППЗУ 13 персонального криптозащитного комплекса отправителя 34 производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ 13 персонального криптозащитного комплекса получателя 35 упомянутый электронный документ автоматически удаляют. В случае, если пользователь даёт подтверждение на отправление пароля 63 в течение периода времени T2, то данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс 35 получателя, при этом упомянутый электронный документ автоматически удаляют из ППЗУ 13 персонального криптозащитного комплекса отправителя 34, а в ППЗУ 13 персонального криптозащитного комплекса 35 получателя после получения им пароля подтверждения передачи электронного документа находят в ППЗУ 13 заблокированный электронный документ и записанную копию пароля подтверждения загрузки 62 электронного документа, отмеченные номером N2, соответствующим номеру, полученному с паролем, и только в случае наличия заблокированного электронного документа, совпадения номеров и наличия прямой связи между паролями автоматически производят разблокирование упомянутого электронного документа; после этого записывают электронный документ в отдел ППЗУ 13 персонального криптозащитного комплекса 35, предназначенный для не копируемых электронных документов и закрытый для пользователей ППЗУ, и удаляют упомянутый временный индивидуальный номер N2. В случае сбоев при передаче электронного документа или паролей подтверждения пользователи осуществляют дублирование передачи.

Номер N1, соответствующий индивидуальному номеру 19 персонального криптозащитного комплекса третьего лица, используется в том случае, когда пароль подтверждения передачи электронного документа предполагается отправлять с другого персонального криптозащитного комплекса. В этом случае к передаваемому электронному документу добавляют индивидуальный номер N1 – 19 персонального криптозащитного комплекса, с которого будут осуществлять отправление пароля подтверждения передачи электронного документа, временный индивидуальный номер N2, формируемый генератором случайных чисел 20, и бесконечное значение периода времени T2, вводимое пользователем, которые шифруют вместе с электронным документом; вводят команду передать электронный документ другому пользователю в процессе защищённого сеанса связи; по окончании передачи данного электронного документа производят его блокирование на заранее определённый период времени T1 в ППЗУ 13 отправителя и отмечают его присвоенным упомянутым номером N2. Принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации; осуществляют поиск и выделение служебной

информации 54 из дешифрованной информации с помощью служебных символов 47, находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа и номера данного документа, записывают электронный документ в отдел ППЗУ 13, предназначенный для некопируемых электронных документов, отмечают его присвоенным номером N2 и блокируют электронный документ на заранее определённый период времени T1, в персональном криптозащитном комплексе 35 принимающей стороны формируют пароль подтверждения загрузки 62 электронного документа, автоматически добавляют к нему упомянутый номер N2 данного электронного документа и в зашифрованном виде передают пароль подтверждения загрузки 62 электронного документа в персональный криптозащитный комплекс 34 отправляющей стороны в процессе того же или другого защищённого сеанса связи; принимают пароль подтверждения загрузки 62 электронного документа в персональном криптозащитном комплексе 34 отправляющей стороны, находят в ППЗУ 13 заблокированный электронный документ, отмеченный номером N2, соответствующим номеру, полученному с паролем и в случае наличия заблокированного электронного документа и совпадения номеров удаляют из ППЗУ 13 данный электронный документ, так как период времени T2 равен бесконечному значению; в персональном криптозащитном комплексе, индивидуальный номер 19 которого соответствует номеру N1, присвоенному электронному документу, вводят числовое значение, соответствующее номеру N2 электронного документа, формируют пароль подтверждения передачи электронного документа 63, автоматически включая в него свой индивидуальный номер 19, соответствующий N1, и введённый номер N2. Данный пароль 63 в зашифрованном виде отправляют в персональный криптозащитный комплекс 35 получателя электронного документа; в ППЗУ 13 персонального криптозащитного комплекса получателя 35 после получения им пароля подтверждения передачи электронного документа находят в ППЗУ 13 заблокированный электронный документ, отмеченный номером N2, соответствующим номеру, полученному с паролем, сверяют номера N1, находящиеся в электронном документе и в пароле, и только в случае совпадения номеров автоматически производят разблокирование упомянутого электронного документа; после чего записывают электронный документ в отдел ППЗУ 13 персонального криптозащитного комплекса 35, предназначенный для не копируемых электронных документов, и удаляют добавленные номера N1 и N2.

Следующий способ передачи электронного документа, защищённого от копирования, отличается тем, что пользователем вводится произвольный период времени T1, бесконечное значение периода времени T2 и добавляется временный индивидуальный номер N2, формируемый генератором случайных чисел 20. В данном способе пароль подтверждения передачи 62 электронного документа отсутствует. А пароль подтверждения передачи электронного документа 63 работает как самостоятельный электронный документ, который может свободно передаваться от пользователя к пользователю в режиме защиты от копирования

с обязательным автоматическим удалением из кассеты персонального криптозащитного комплекса, с которого данный пароль передаётся.

Для формирования пароля подтверждения передачи 63 электронного документа вводят команду сформировать пароль подтверждения передачи данного электронного документа; формируют пароль подтверждения электронного документа, присваивают ему номер и, при наличии, переменный номинал, соответствующие временному номеру и переменному номиналу электронного документа; передают пароль подтверждения электронного документа в процессе криптозащитного сеанса связи в зашифрованном виде определённому пользователю либо оставляют в своём персональном криптозащитном комплексе 34.

В данном способе электронный документ блокируется в течение периода времени T1 в ППЗУ 13 персонального криптозащитного комплекса отправителя, но при этом электронный документ может неограниченно копироваться и распространяться другим пользователям в процессе криптозащитных сеансов связи либо в электронных письмах с соответствующей пометкой о том, что получаемый другими пользователями электронный документ является копией. По окончании периода времени T1 удаляют электронный документ из ППЗУ 13 отправителя 34; принимают копии электронного документа, производят дешифрование электронного документа, осуществляют поиск и выделение служебной информации 54 из дешифрованной информации с помощью служебных символов 47; находят пометку о том, что это копия электронного документа, временный индивидуальный номер N2 данного документа, записывают электронный документ в отдел ППЗУ 13 и отмечают его присвоенным временным индивидуальным номером N2. В персональном криптозащитном комплексе одного из пользователей, принявших копию электронного документа принимают пароль подтверждения передачи 63 электронного документа, находят в ППЗУ 13 копию электронного документа, отмеченную номером N2, соответствующим номеру N2, полученному с паролем 63; и в случае совпадения номеров снимают с копии электронного документа пометку о том, что это копия электронного документа, после чего записывают электронный документ в отдел ППЗУ 13 персонального криптозащитного комплекса, предназначенный для некопируемых электронных документов и закрытый для пользователей ППЗУ, и удаляют упомянутый временный индивидуальный номер N2. В персональном криптозащитном комплексе отправителя пароля подтверждения передачи электронного документа после осуществления передачи данного пароля автоматически производят его удаление из ППЗУ 13, а в случае передачи части пароля с переменным номиналом в оставшейся в ППЗУ 13 части пароля уменьшают его номинал на сумму, равную переданной части.

Персональный криптозащитный комплекс позволяет осуществлять процедуру одновременного обмена электронными документами, защищёнными от копирования по линии связи с предварительным просмотром электронных документов. Для этого синхронно формируют одноразовый ключ шифрования 38 (фиг.12) на основе выработанных в

персональных криптозащитных комплексах 34 и 35 пользователей случайных числах 36 и 37; синхронно формируют динамически преобразуемые дочерние коды 39 на основе материнского кода 15 и одноразового ключа шифрования 38 в персональных криптозащитных комплексах пользователей; вводят исходную информацию в каждый из персональных криптозащитных комплексов пользователей; формируют с помощью программы обработки информации в соответствии с установленным режимом обработки пользовательской информации и ранее полученной информации служебную информацию, объединяют ее с обработанной пользовательской информацией, получая электронный документ 60, причем атрибуты электронного документа в виде служебной информации 54 выделяют от обработанной пользовательской информации предварительно определенными служебными символами 47, и в соответствии с командой пользователя - сформировать электронный документ, защищённый от копирования, включают в служебную информацию определённую команду для персональных криптозащитных комплексов в виде типового набора символов, заранее введённых в ПЗУ в составе программы обработки информации, и сохраняют полученный электронный документ в отделе ППЗУ, предназначенном для не копируемых электронных документов, персонального криптозащитного комплекса. По меньшей мере в одном из персональных криптозащитных комплексов вводят команду 76 одновременного обмена электронными документами и посылают данную команду в виде зашифрованного с помощью выработанного одноразового ключа шифрования сигнала 77 в другой персональный криптозащитный комплекс 35; в каждом из персональных криптозащитных комплексов вводят команду пользователя начать передачу записанного в ППЗУ 13 некопируемого электронного документа 60 и 75 другому абоненту установленного сеанса связи; шифруют динамически преобразуемым дочерним кодом электронный документ, считывая при этом из служебной информации команду о некопируемости электронного документа, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в другой персональный криптозащитный комплекс; в соответствии с командой 76 об одновременном обмене электронных документов по окончании передачи некопируемого электронного документа производят его блокирование 61 и 78 на заранее определённый период времени T1 в ППЗУ 13 отправителя; принимают электронный документ и производят дешифрование электронного документа; устанавливают достоверность информации путём проверки на отсутствие искажений в информации, осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов; находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа; записывают электронный документ в отдел ППЗУ, предназначенный для некопируемых электронных документов, блокируют его на заранее определённый период времени T1 и выводят полученный электронный документ пользователю для ознакомления. В персональном криптозащитном комплексе принимающей

стороны формируют пароль подтверждения загрузки 62 электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны. В случае неполучения отправителем от получателя пароля подтверждения загрузки электронного документа в течение периода времени T1 производят разблокирование электронного документа в ППЗУ персонального криптозащитного комплекса отправителя. В случае не отправления получателем отправителю пароля подтверждения загрузки электронного документа в течение периода времени T1 производят удаление электронного документа из ППЗУ 13 персонального криптозащитного комплекса получателя; принимают пароль подтверждения загрузки 62 электронного документа в персональном криптозащитном комплексе отправляющей стороны, формируют пароль подтверждения передачи 63 электронного документа и запрашивают подтверждение 79 пользователя на отправление данного пароля в персональный криптозащитный комплекс принимающей стороны. В случае если пользователь не даёт подтверждение на отправление пароля в течение заранее определённого периода времени T2, то по истечении данного периода времени в ППЗУ персонального криптозащитного комплекса отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ персонального криптозащитного комплекса получателя упомянутый электронный документ автоматически удаляют. В случае если пользователь даёт подтверждение 79 на отправление пароля в течение периода времени T2, то отправляют другому пользователю в зашифрованном виде заранее определённый сигнал 80, содержащий информацию о данном подтверждении, и получают аналогичный сигнал от упомянутого пользователя. После обмена подтверждающими сигналами 80 производят синхронизацию по последнему сигналу и с момента отправления в одном из персональных криптозащитных комплексов и соответственно получения в другом персональном криптозащитном комплексе последнего бита упомянутого сигнала начинают процедуру одновременного обмена в зашифрованном виде паролями подтверждения передачи 63 электронного документа, причём в каждом из персональных криптозащитных комплексах контролируют получение сигнала, содержащего пароль от противоположной стороны, и в случае отсутствия или прерывания данного сигнала прекращают передачу своего пароля. После отправления пароля подтверждения передачи 63 упомянутый электронный документ автоматически удаляют из ППЗУ персонального криптозащитного комплекса отправителя, а в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа автоматически производят разблокирование упомянутого электронного документа.

Для повышения безопасности при обмене электронными документами, защищёнными от копирования 60 и 75, в последний подтверждающий сигнал 80 автоматически вводят значение времени T, отличающееся от текущего показания времени на период времени t, значение которого формируется с помощью генератора случайных чисел 20; отправляют

данный сигнал другому пользователю и по истечении отправления сигнала до наступления времени Т передают случайный сигнал, формируемый генератором случайных чисел 20; при наступлении времени Т автоматически прекращают передачу случайного сигнала и начинают одновременную передачу в зашифрованном виде паролей подтверждения передачи 63 электронных документов, причём случайный сигнал и криптограмма паролей имеют одинаковые характеристики. Данный приём позволяет избежать умышленного сбоя при передаче последних байтов паролей подтверждения передачи электронных документов, так как время окончания передачи в этом случае становится неизвестным.

Следующий способ позволяет гарантировать одновременное подписание электронного документа по меньшей мере двумя пользователями по линии связи электронными цифровыми подписями. Для этого пользователи обмениваются копией электронного документа 60, которую предварительно подписывают каждый своей электронной цифровой подписью, и после получения, блокирования в ППЗУ 13 и ознакомления с полученными электронными документами, по меньшей мере одним из пользователей вводится команда одновременного подписания данного электронного документа; посылается сигнал в зашифрованном виде другому пользователю, содержащий информацию об одновременном подписании электронного документа и выводится пользователю; после обмена паролями подтверждения передачи 63 электронных документов в каждом из персональных криптозащитных комплексов 34 и 35 автоматически производят подписание полученных электронных документов электронной цифровой подписью пользователя. Команда об одновременном подписании электронного документа после его обоюдного подписания позволяет снять с данного электронного документа защиту от копирования для свободного ознакомления с данным электронным документом любым пользователем.

Программа обработки информации 22 (фиг.14) персональных криптозащитных комплексов позволяет передавать сообщения в режиме электронных писем с уведомлением о получении электронного сообщения адресатом. При этом гарантируется, что адресат сможет прочитать сообщение только при условии получения отправителем электронного уведомления с электронной подписью адресата о получении им данного электронного письма. Для этого в состав программы обработки информации 22 заранее введена типовая форма бланка уведомления, в который автоматически заносятся номер электронного письма, формируемый перед его отправлением генератором случайных чисел 20 и электронная подпись пользователя – получателя электронного письма. Сообщение, которое сначала получает адресат, находится в зашифрованном виде, из которого персональный криптозащитный комплекс получателя дешифрует служебную часть сообщения, содержащую номер электронного письма и информацию о том, что данное сообщение является электронным письмом с уведомлением. Процедура отправления и получения электронного письма с уведомлением выглядит следующим образом: в одном из персональных криптозащитных комплексов 34 вводят команду

86 отправить электронное письмо с уведомлением, вводят информацию; добавляют к данной информации номер N - 88, сформированный генератором случайных чисел 20, выделяют его заранее введёнными служебными символами 47 и шифруют информацию с номером с применением пароля дешифрования 48; в соответствии с упомянутой командой 86 записывают пароль дешифрования 48 в ППЗУ 13 персонального криптозащитного комплекса 34 и отмечают его упомянутым номером 88; формируют электронное письмо с уведомлением из введённой зашифрованной информации 45 и добавленной к ней служебной информации 54, отделённой заранее введёнными служебными символами 47, в которой содержится номер 88, соответствующий номеру информации и пароля дешифрования 48, и введена команда о том, что данная информация является электронным письмом с уведомлением. Копию зашифрованного электронного письма с уведомлением выводят для записи на носитель, устанавливают криптозащитный сеанс связи с определённым пользователем 35 с применением персональных криптозащитных комплексов и передают электронное письмо с уведомлением 87, принимают информацию, дешифруют служебную информацию, находят номер 88, который записывают в ППЗУ 13, команду о том, что полученная зашифрованная информация является электронным письмом с уведомлением, и выводят данную команду пользователю 89. В соответствии с упомянутой командой и вводимой получателем командой 90 – отправить уведомление о получении данного сообщения отправителю, формируют электронный документ в виде заранее введённого типового бланка уведомления 92; вводят в него номер 88, соответствующий номеру полученной информации, и подписывают данный электронный документ электронной подписью пользователя 24, содержащей текущие дату и время; отправляют другому пользователю в зашифрованном виде заранее определённый сигнал 91, содержащий информацию, подтверждающую наличие уведомления. После отправления и соответственно получения упомянутого сигнала 91 производят одновременный обмен электронного бланка уведомления 92 на пароль дешифрования 48 электронного письма, принимают пароль дешифрования 48 в персональный криптозащитный комплекс 35 получателя, с его помощью расшифровывают информацию, полученную в электронном письме с уведомлением 87 и выводят пользователю; принимают электронный документ, являющийся бланком уведомления о получении электронного письма с уведомлением в персональный криптозащитный комплекс 34 отправителя; расшифровывают его и выводят пользователю, а криптограмму бланка уведомления записывают на носитель.

В случае использования электронной почты для отправления электронного письма с уведомлением используется узловой компьютер (сервер) с подключённым к нему узловым криптозащитным комплексом. Далее в персональном криптозащитном комплексе отправителя 34 вводят команду отправить электронное письмо с уведомлением, вводят информацию, добавляют к данной информации номер N - 88, сформированный генератором случайных чисел 20, выделяют его заранее введёнными служебными символами 47, вводят индивидуальный

номер I – 19 персонального криптозащитного комплекса адресата, генерируют случайное число Z – 36; на основе введённого номера I и случайного числа Z формируют одноразовый ключ шифрования 38 и шифруют информацию, включая добавленный случайный номер N – 88; в соответствии с упомянутой командой записывают случайное число Z в ППЗУ 13 персонального криптозащитного комплекса 34 и отмечают его упомянутым случайным номером N; формируют электронное письмо с уведомлением из введённой зашифрованной информации и добавленной к ней служебной информации, отделённой заранее введёнными служебными символами 47, в которой содержится номер, соответствующий номеру N информации, и введена команда о том, что данная информация является электронным письмом с уведомлением, копию зашифрованного электронного письма с уведомлением выводят для записи на носитель; передают электронное письмо с уведомлением в узловой компьютер, устанавливают криптозащитный сеанс связи с узловым криптозащитным комплексом, подключенным к узловому компьютеру, передают случайное число Z – 36, которое сохраняют в узловом криптозащитном комплексе; принимают электронное письмо с уведомлением с узлового компьютера в персональный криптозащитный комплекс 35 адресата, дешифруют служебную информацию, находят номер N, который записывают в ППЗУ 13, команду о том, что полученная зашифрованная информация является электронным письмом с уведомлением, и выводят данную команду пользователю. В соответствии с упомянутой командой и вводимой получателем командой – отправить уведомление о получении данного сообщения отправителю, формируют электронный документ в виде заранее введённого типового бланка уведомления, вводят в него номер N, соответствующий номеру полученной информации, и подписывают данный электронный документ электронной подписью пользователя, содержащей текущие дату и время; отправляют в узловой криптозащитный комплекс через узловой компьютер в зашифрованном виде заранее определённый сигнал, содержащий информацию, подтверждающую наличие уведомления; после отправления и соответственно получения упомянутого сигнала производят одновременный обмен электронного бланка уведомления на случайное число Z – 36; принимают случайное число Z – 36 в персональный криптозащитный комплекс 35 получателя, выводят из ПЗУ 17 индивидуальный номер I – 19 персонального криптозащитного комплекса и на их основе формируют одноразовый ключ 38 дешифрования; расшифровывают информацию, полученную в электронном письме с уведомлением и выводят пользователю. В персональном криптозащитном комплексе 34 отправителя принимают с узлового криптозащитного комплекса через узловой компьютер электронный документ, являющийся бланком уведомления о получении электронного письма с уведомлением в персональный криптозащитный комплекс отправителя, расшифровывают его и выводят пользователю, а криптограмму бланка уведомления записывают на носитель.

Применение персональных криптозащитных комплексов, для расчётов электронными банковскими векселями и электронными наличными деньгами, позволяет конвертировать

данные средства расчёта в электронные деньги несовместимых платёжных систем. Причём, в целях безопасности, процедура конвертации носит однонаправленный характер, т.е. обратное конвертирование электронных денег с пластиковых карт в электронные наличные деньги или электронные векселя нежелательно. Для осуществления процедуры конвертации пользователю потребуется устройство считывания с пластиковых карт, совместимое с персональным криптозащитным комплексом. Кроме того, данная процедура осуществима только после определённых взаимодействий персональных криптозащитных комплексов пользователя и банка, клиентом которого является пользователь, а именно, если предполагается конвертировать электронные наличные деньги или бессрочные электронные банковские векселя:

с помощью заранее заложенной программы в составе программы обработки информации 22 в персональном криптозащитном комплексе банка формируют электронный документ с применением заранее определённых служебных символов 47, предназначенный для определённого пользователя, в который включают подписанную банком электронную банкноту, условия банка в виде определённых команд; устанавливают криптозащитный сеанс связи с применением персональных криптозащитных комплексов между банком и пользователем и передают пользователю сформированный электронный документ. Принимают в персональный криптозащитный комплекс пользователя упомянутый электронный документ, расшифровывают, определяют служебные символы 47, с их помощью определяют команды и электронную банкноту, подписанную банком, записывают электронную банкноту в ППЗУ 13 персонального криптозащитного комплекса и блокируют до получения определённых команд и выполнения условий банка, содержащихся в полученных командах электронного документа. Принимают в персональный криптозащитный комплекс пользователя электронные наличные деньги или электронные банковские векселя, вводят команду пользователя разблокировать электронную банкноту, подписанную банком; в соответствии с командой пользователя проверяют наличие в ППЗУ 13 электронных наличных денег или электронных банковских векселей и их соответствие условиям банка по сумме, валюте и другим атрибутам, при выполнении условий банка производят блокирование определённой данным условием суммы электронных наличных денег или электронных банковских векселей и одновременное разблокирование электронной банкноты, причём сумма блокируемых электронных наличных денег или векселей в соответствии с условиями банка может превышать сумму электронной банкноты. Подключают к персональному криптозащитному комплексу пользователя посредством терминала 2 носитель (пластиковую карту) и производят передачу электронной банкноты на данный носитель, производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя; в банке принимают данную электронную банкноту, заносят её в регистр; в случае если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя, выставляют на банковский счёт

пользователя счёт на сумму потраченной электронной банкноты за вычетом сдачи с момента проведения транзакции платежа и одновременно вводят информацию о сумме кредита в персональный криптозащитный комплекс банка в виде заранее определённых команд. Подключают персональный криптозащитный комплекс пользователя к персональному криптозащитному комплексу банка, устанавливают между ними криптозащитный сеанс связи, идентифицируют персональные криптозащитные комплексы и вводят команду на погашение кредита; производят расчёт суммы для разблокирования в соответствии с суммой и сроком кредита; разблокируют определённую расчётом сумму электронных наличных денег или электронных банковских векселей; необходимую для погашения кредита сумму передают в персональный криптозащитный комплекс банка, а оставшаяся часть разблокированной суммы остаётся в распоряжении пользователя.

В случае если предполагается конвертировать срочные или бессрочные электронные банковские векселя, то осуществляют следующие процедуры. С помощью заранее заложенной программы в составе программы обработки информации 22 в персональном криптозащитном комплексе банка формируют электронный документ с применением заранее определённых служебных символов 47, предназначенный для определённого пользователя, в который включают подписанную банком электронную банкноту, условия банка в виде определённых команд; устанавливают криптозащитный сеанс связи с применением персональных криптозащитных комплексов между банком и пользователем, и передают пользователю сформированный электронный документ; принимают в персональный криптозащитный комплекс пользователя упомянутый электронный документ, расшифровывают, определяют служебные символы 47, с их помощью определяют команды и электронную банкноту, подписанную банком; записывают электронную банкноту в ППЗУ 13 персонального криптозащитного комплекса и блокируют до получения определённых команд и выполнения условий банка, содержащихся в полученных командах электронного документа. Принимают в персональный криптозащитный комплекс пользователя электронные банковские векселя с персонального криптозащитного комплекса другого пользователя, вводят команду пользователя разблокировать электронную банкноту, подписанную банком. В соответствии с командой пользователя проверяют наличие в ППЗУ 13 электронного банковского векселя и его соответствие условиям банка по сумме, валюте и другим атрибутам; считывают с электронного векселя данные пользователя 24, на имя которого был выписан электронный вексель, включая индивидуальный номер 19 его персонального криптозащитного комплекса. Если электронный вексель отвечает условиям банка, то производят разблокирование электронной банкноты с одновременным уменьшением номинала упомянутого электронного векселя на сумму, соответствующую сумме электронной банкноты, при этом к электронной банкноте добавляют зашифрованную информацию, содержащую данные пользователя 24 и 19, взятые из упомянутого электронного векселя; подключают к персональному криптозащитному

комплексу пользователя посредством терминала 2 носитель (пластиковую карту) и производят передачу электронной банкноты на данный носитель. Производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя; в банке принимают данную электронную банкноту, дешифруют добавленную к ней информацию; определяют по данной информации счёт пользователя, на котором хранится залоговая сумма под упомянутый электронный вексель, и списывают с него сумму, соответствующую полученной электронной банкноте; заносят электронную банкноту в регистр, и если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя.

При совпадении данных пользователя 24, включая индивидуальный номер 19 его персонального криптозащитного комплекса, содержащихся в электронном векселе, с аналогичными данными в ПЗУ 17 персонального криптозащитного комплекса пользователя производят разблокирование электронной банкноты, включающей в себя номер счёта пользователя, с одновременным уменьшением номинала упомянутого электронного векселя на сумму, соответствующую сумме электронной банкноты; подключают к персональному криптозащитному комплексу пользователя посредством терминала носитель и производят передачу электронной банкноты на данный носитель без добавления к электронной банкноте дополнительных данных.

Производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя, в банке принимают данную электронную банкноту, определяют по ней счёт пользователя, на котором хранится залоговая сумма под упомянутый электронный вексель, и списывают с него сумму, соответствующую полученной электронной банкноте; заносят электронную банкноту в регистр, и если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя.

Промышленная применимость

Система может быть реализована на базе RISC процессора, а для защиты компьютерных программ от несанкционированного копирования на базе процессоров Intel 80x86. Система в целом может быть реализована на базе IBM PC путём встраивания микропроцессора, ОЗУ, часов и аккумулятора персонального компьютера в защитную оптическую оболочку, снабжённую встроенным криптоядром.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ шифрования и дешифрования с использованием персональных криптозащитных комплексов, включающий следующие этапы, осуществляемые в каждом из персональных криптозащитных комплексов:

а) сохранение в ПЗУ каждого из персональных криптозащитных комплексов копий материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутые персональные криптозащитные комплексы, исключающим возможность копирования материнского кода на другие носители и изменения программного кода упомянутых программ,

б) подключение по меньшей мере двумя пользователями своих персональных криптозащитных комплексов к линии связи и установление ими количества участников криптозащитного сеанса связи,

в) выработка случайного числа Z персональным криптозащитным комплексом и его сохранение в оперативной памяти,

г) обмен по линии связи данными выработанных случайных чисел Z между упомянутыми персональными криптозащитными комплексами с установлением момента времени запуска формирования одноразового ключа сеанса связи,

д) синхронное формирование одноразового ключа сеанса связи X путём считывания из оперативной памяти сохраненного случайного числа Z, выполнения заранее определённой арифметической операции над случайным числом Z, считанным из оперативной памяти, и случайным числом Z', полученным от другого пользовательского криптозащитного устройства, для получения результирующего числа X и сохранение результирующего числа X в оперативной памяти,

е) синхронное формирование динамически преобразуемого дочернего кода в персональных криптозащитных комплексах на основе материнского кода и одноразового ключа сеанса связи,

ж) ввод и разделение исходной передаваемой информации на пакеты определенного размера и шифрование пакетов с использованием динамически преобразуемого дочернего кода,

з) передача зашифрованных пакетов информации по меньшей мере в один другой персональный криптозащитный комплекс,

и) прием зашифрованных пакетов информации в упомянутом по меньшей мере одном другом персональном криптозащитном комплексе,

к) дешифрование принятых зашифрованных пакетов с использованием динамически преобразуемого дочернего кода,

л) объединение дешифрованных пакетов в исходную информацию,

и повторение этапов (е)-(л) для передачи информации в обратном направлении в том же сеансе связи.

2. Способ по п.1, отличающийся тем, что момент времени запуска формирования одноразового ключа сеанса связи устанавливают по моменту передачи и приема данных, соответствующих последнему из обмениваемых по линии связи на этапе (г) упомянутых случайных чисел.

3. Способ по п.1, отличающийся тем, что одновременно с формированием одноразового ключа сеанса связи в каждом из персональных криптозащитных комплексах формируют одноразовый пароль подтверждения установления защищённого сеанса связи, который совпадает у данных участников сеанса связи и с помощью которого удостоверяются в установлении защищённого сеанса связи.

4. Способ по п. 1, отличающийся тем, что преобразование динамического дочернего кода на этапах (ж) и (к) синхронизируют по моменту передачи и приема каждого из пакетов информации.

5. Способ по п 1, отличающийся тем, что при осуществлении дуплексной связи с использованием персональных криптозащитных комплексов в каждом из них

синхронно формируют два динамически преобразуемых дочерних кода на основе материнского кода и одноразового ключа сеанса связи,

вводят и разделяют исходную передаваемую информацию на пакеты определенного размера и шифруют пакеты с использованием первого динамически преобразуемого дочернего кода,

передают зашифрованные пакеты информации в другой персональный криптозащитный комплекс,

принимают зашифрованные пакеты информации в упомянутом другом персональном криптозащитном комплексе и дешифруют принятые зашифрованные пакеты с использованием второго динамически преобразуемого дочернего кода,

причем, если для одного из персональных криптозащитных комплексов первый динамически преобразуемого дочерний код используется для шифрования информации, то для другого персонального криптозащитного комплекса упомянутый динамически преобразуемый дочерний код используется для дешифрования информации и соответственно считается вторым динамически преобразуемым дочерним кодом,

при этом преобразование первого динамически преобразуемого дочернего кода на этапах (ж) и (к) синхронизируют по моменту передачи каждого из пакетов информации, а для второго динамически преобразуемого дочернего кода преобразование на этапах (ж) и (к)

синхронизируют по моменту приёма каждого из пакетов информации, таким образом, синхронизация каждой пары динамически преобразуемых дочерних кодов осуществляется независимо от другой пары.

6. Способ шифрования и дешифрования информации с использованием персональных криптозащитных комплексов, при котором

сохраняют в ПЗУ каждого из персональных криптозащитных комплексов копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутые персональные криптозащитные комплексы, исключающим возможность копирования материнского кода на другие носители и изменения программного кода упомянутых программ, сохраняют в ПЗУ индивидуальный номер I персонального криптозащитного комплекса,

в персональном криптозащитном комплексе, являющемся отправителем информации,

вырабатывают случайное число Z и сохраняют его в оперативной памяти,

вводят индивидуальный номер I персонального криптозащитного комплекса получателя информации,

формируют одноразовый ключ шифрования путем считывания из оперативной памяти сохраненного случайного числа Z и индивидуального номера I, выполняют арифметическую операцию над случайным числом Z и индивидуальным номером I для получения результирующего числа X и сохраняют результирующее число X в оперативной памяти,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования,

вводят и разделяют отправляемую информацию на пакеты определенного размера и шифруют пакеты с использованием динамически преобразуемого дочернего кода и

выводят зашифрованные пакеты информации для записи на носитель совместно со случайным числом Z для дальнейшей передачи получателю, при этом преобразование динамического дочернего кода производится по моменту окончания шифрования заранее определенного количества байтов информации,

в персональном криптозащитном комплексе, являющемся получателем информации,

считывают из ПЗУ индивидуальный номер I персонального криптозащитного комплекса получателя информации и сохраняют его в оперативной памяти,

вводят в оперативную память число Z, полученное от отправителя информации,

формируют одноразовый ключ шифрования путем считывания из оперативной памяти сохраненного случайного числа Z и индивидуального номера I, выполняют арифметическую операцию над случайным числом Z и индивидуальным номером I для

получения результирующего случайного числа X и сохраняют результирующее случайное число X в оперативной памяти,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования,

вводят зашифрованные пакеты информации с носителя и дешифруют пакеты с помощью динамического дочернего кода, при этом преобразование динамического дочернего кода производится по моменту окончания дешифрования заранее определенного количества байтов информации, и

объединяют пакеты и выводят дешифрованную информацию получателю информации.

7. Способ шифрования и дешифрования электронного документа с использованием персонального криптозащитного комплекса, при котором

сохраняют в ПЗУ каждого из персональных криптозащитных комплексов копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутые персональные криптозащитные комплексы, исключающим возможность копирования материнского кода на другие носители и изменения программного кода упомянутых программ, устанавливают дату и время во встроенных часах,

по меньшей мере в одном персональном криптозащитном комплексе, являющемся одной из сторон формирования электронного документа,

вырабатывают по команде пользователя пароль дешифрования в виде случайного числа Y и случайное число Z, получают случайное число Z' или число I и сохраняют упомянутые числа в оперативной памяти,

вводят пароль дешифрования в начало электронного документа и выделяют его особым образом от основного текста электронного документа,

формируют одноразовый ключ шифрования X на основе считанных из оперативной памяти упомянутых случайных чисел Z, Z' или числа I и выводят пользователю числа Z и Y,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования,

шифруют пароль дешифрования с использованием динамически преобразуемого дочернего кода,

вводят и разделяют исходную информацию на пакеты определенного размера и шифруют пакеты с использованием динамически преобразуемого дочернего кода,

выводят зашифрованные пакеты информации, включающей зашифрованный пароль дешифрования, для передачи вместе с числами Y, Z, Z' или I персональным криптозащитным комплексам других пользователей или для записи на носители,

по меньшей мере, в любой персональный криптозащитный комплекс, вводят случайные числа Z, Z' или число I и сохраняют их в оперативной памяти персонального криптозащитного комплекса , вводят команду на дешифрование и вводят пароль дешифрования Y,

формируют одноразовый ключ дешифрования X на основе считанных из оперативной памяти упомянутых случайных чисел Z, Z' или числа I,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа дешифрования,

вводят зашифрованные пакеты информации, выделяют из них пароль дешифрования, дешифруют его и сравнивают с введенным пользователем паролем дешифрования,

в случае совпадения осуществляют дешифрование зашифрованных пакетов информации и выводят пользователю дешифрованный исходный электронный документ, а при несовпадении - прекращают дешифрование.

8. Способ по п. 7, отличающийся тем, что сравнение выделенного пользователем и введенного пароля дешифрования осуществляют путем шифрования введенного пользователем пароля дешифрования в виде случайного числа Y с помощью сформированного динамически преобразуемого дочернего кода и сравнения зашифрованного числа Y с выделенным зашифрованным паролем дешифрования.

9. Способ по п. 7, отличающийся тем, что случайное число Z' получают от другого пользовательского криптозащитного комплекса в процессе обмена по линии связи выработанными случайными числами Z.

10. Способ по п. 7, отличающийся тем, что в качестве числа I используют индивидуальный номер персонального криптозащитного комплекса, являющегося одним из получателей электронного документа.

11. Способ шифрования и дешифрования электронного документа с использованием персонального криптозащитного комплекса, при котором

сохраняют в ПЗУ каждого из персональных криптозащитных комплексов копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутые персональные криптозащитные комплексы, исключающим возможность копирования материнского кода на другие носители и изменения программного кода упомянутых программ, устанавливают дату и время во встроенных часах,

в одном персональном криптозащитном комплексе, формирующем электронный документ,

вырабатывают по команде пользователя пароль дешифрования с помощью генератора случайных чисел в виде случайного числа X определённой разрядности, сохраняют его в оперативной памяти и выводят его пользователю,

формируют одноразовый ключ шифрования X на основе считанного из оперативной памяти случайного числа X,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования,

вводят и разделяют исходную информацию на пакеты определенного размера и шифруют пакеты с использованием динамически преобразуемого дочернего кода,

выводят зашифрованные пакеты информации для передачи персональным криптозащитным комплексам других пользователей или для записи на носители;

по меньшей мере в одном любом персональном криптозащитном комплексе

вводят пароль дешифрования в виде случайного числа X определённой разрядности и команду дешифрования,

формируют одноразовый ключ дешифрования X на основе считанного из оперативной памяти случайного числа X,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа дешифрования,

вводят зашифрованные пакеты информации, дешифруют зашифрованные пакеты информации и выводят пользователю дешифрованный исходный электронный документ.

12. Способ по п. 7 или 11, отличающийся тем, что по меньшей мере в одном персональном криптозащитном комплексе, являющемся одной из сторон формирования электронного документа,

пользователь вводит команду применить пароль дешифрования и вводит через устройство ввода информации любой набор символов который предполагает использовать в качестве пароля дешифрования и который представляют в виде числа D,

затем с помощью генератора случайных чисел вырабатывают случайное число, используемое в качестве пароля дешифрования и затем совершают определённую обратимую арифметическую операцию между упомянутым случайным числом и числом D, получая в итоге число F, которое выводят пользователю вместе с зашифрованным электронным документом для передачи персональным криптозащитным комплексам других пользователей или для записи на носители,

по меньшей мере в одном любом персональном криптозащитном комплексе, вводят число F, вводят пароль дешифрования D, совершают между данными числами определённую арифметическую операцию, сохраняют полученный результат в оперативной памяти персонального криптозащитного комплекса и используют его для дешифрования вводимой информации.

13. Способ по п. 7 или 11, отличающийся тем, что пароль дешифрования формируется с включением в него команд, адресованных персональным криптозащитным

комплексам и устанавливающих дату и время дешифрования электронного документа, только по истечении которых персональный криптозащитный комплекс любого пользователя, дешифрующего электронный документ, произведёт его дешифрование, а также включением заранее определённых команд, позволяющих вносить определённые изменения в содержание электронного документа.

14. Способ по п. 1, 6, 7 или 11 отличающийся тем, что при формировании динамически преобразуемого дочернего кода

e.1) считывают из оперативной памяти число X, считывают из памяти материнского кода первое число M1 материнского кода, выполняют арифметическую операцию над считанными числами X и M1 для получения первого результирующего числа определённой разрядности, которое сохраняют в оперативной памяти, причём отделяют от данного числа k – младших разрядов и присваивают полученному числу P1 номер, соответствующий отделённому числу k-ной разрядности,

e.2) считывают из оперативной памяти упомянутое первое число P1, считывают из памяти материнского кода второе число M2 материнского кода, выполняют арифметическую операцию над считанными числами P1 и M2 для получения второго числа P2 и сохраняют упомянутое число P2 в оперативной памяти,

e.3) повторяют этап (e.2) для чисел P(i-1) и Mi, где i = 3,..., N, для получения множества чисел P3...PN, сохраненных в оперативной памяти,

e.4) формируют из множества чисел P1...PN два подмножества, первое из которых состоит из чисел, соответствующих k младшим разрядам чисел P1...PN, а второе – из чисел, соответствующих m старшим разрядам чисел P1...PN, группируют второе подмножество чисел в таблицу по адресам, соответствующим числам первого подмножества, количество которых равно возможному количеству чисел первого подмножества,

e.5) выбирают столбец таблицы с максимальным количеством чисел из второго подмножества или все столбцы с одинаковым максимальным количеством чисел и производят последовательно арифметическую операцию с последовательными парами чисел выбранных столбцов, в результате чего получают промежуточное число K,

e.6) повторяют для числа K и множества чисел P1...PN этапы (e.1) – (e.4), причем на этапе (e.4) выбирают k = 8 бит и полученные числа второго подмножества распределяют в таблицу с 256 столбцами, пронумерованными одним из 256 байтов, причем столбцы с количеством чисел менее двух дополняют числами из столбцов с максимальным количеством чисел,

e.7) производят последовательно арифметическую операцию с последовательными парами чисел столбцов, для получения для каждого столбца числа Q1... Q256 определенной разрядности,

е.8) формируют из множества чисел Q1...Q256 два подмножества, первое из которых состоит из чисел, соответствующих 4 младшим разрядам чисел Q1...Q256, а второе – из чисел, соответствующих остальным старшим разрядам чисел Q1...Q256, группируют второе подмножество чисел в таблицу размером 100 х 100 по адресам, соответствующим числам первого подмножества,

е.9) формируют таблицу размером 16 х 16 из байтов, соответствующих второму подмножеству чисел пункта (е.8), путем последовательного построчного прохождения таблицы размером 100 х 100, нахождения в ней ячеек с числами упомянутого второго подмножества и записи в той же последовательности в таблицу размером 16 х 16 байтов, соответствующих найденным числам,

е.10) производят арифметические операции над числами второго подмножества пункта (е.8), соответствующими по меньшей мере двум соседним байтам для каждого байта из таблицы размером 16 х 16, для получения двух новых подмножеств и второй таблицы размером 16 х 16, повторяя этапы (е.8) – (е.9),

е.11) после шифрования и дешифрования определенного количества байтов информации с помощью сформированного дочернего кода обновляют первую и вторую таблицы размером 16 х 16 путем удаления первой таблицы, замены ее второй таблицей и формированием новой второй таблицы согласно этапу (е.10).

15. Способ по п. 14, отличающийся тем, что перед началом шифрования и дешифрования информации в каждом персональном криптозащитном комплексе создают несколько таблиц 16 х 16, повторяя этапы (е.8) – (е.9), общим количеством R, заранее определённым и большим двух, и сохраняют их в оперативной памяти, а шифрование и дешифрование пакета информации, состоящего из определенного количества байтов, производят с помощью двух таблиц 16 х 16, начиная с первой и второй таблиц, затем следующий пакет информации шифруют и дешифруют с помощью первой и третьей таблиц и так далее до последней таблицы 16 х 16, которую также используют в паре с первой таблицей,

после чего удаляют первую таблицу, заменят ее второй таблицей, вторую таблицу заменяют третьей таблицей и так далее до последней таблицы, которую ставят на место предпоследней таблицы, а на место последней таблицы ставят новую таблицу 16 х 16, сформированную согласно этапу (е.10), и продолжают шифрование и дешифрование пакетов информации начиная с первой и второй таблиц.

16. Способ по п. 14, отличающийся тем, что при формировании динамически преобразуемого дочернего кода, начиная с этапа (е.6), повторяют для числа К и множества чисел P1...PN этапы (е.1) – (е.4), причем на этапе (е.4) выбирают k = 9 бит и полученные числа второго подмножества распределяют в таблицу с 512 столбцами, пронумерованными одним из 512 байтов, причем столбцы с количеством чисел менее двух дополняют числами из столбцов с максимальным количеством чисел,

е.7) производят последовательно арифметическую операцию с последовательными парами чисел столбцов, для получения для каждого столбца числа Q1... Q512 определенной разрядности,

е.8) формируют из множества чисел Q1...Q512 два подмножества, первое из которых состоит из чисел, соответствующих 6 младшим разрядам чисел Q1...Q512, а второе – из чисел, соответствующих остальным старшим разрядам чисел Q1...Q512, группируют второе подмножество чисел в таблицу размером 100 x 100 x 100 по адресам, соответствующим числам первого подмножества,

е.9) формируют таблицу размером 8 x 8 x 8 из байтов, соответствующих второму подмножеству чисел пункта (е.8), путем последовательного построчного прохождения таблицы размером 100 x 100 x 100, нахождения в ней ячеек с числами упомянутого второго подмножества и записи в той же последовательности в таблицу размером 8 x 8 x 8 байтов, соответствующих найденным числам,

е.10) производят арифметические операции над числами второго подмножества пункта (е.8), соответствующими по меньшей мере двум соседним байтам для каждого байта из таблицы размером 8 x 8 x 8, для получения двух новых подмножеств и второй таблицы размером 8 x 8 x 8, повторяя этапы (е.8) – (е.9),

е.11) после шифрования и дешифрования определенного количества байтов информации с помощью сформированного дочернего кода обновляют первую и вторую таблицы размером 8 x 8 x 8 путем удаления первой таблицы, замены ее второй таблицей и формированием новой второй таблицы согласно пункту (е.10).

17. Способ по п. 14 или 16, отличающийся тем, что арифметические операции с числами производят путем деления одного числа на другое и сохраняют полученный результат в оперативной памяти, затем в полученном числе выделяют n значащих цифр, которые представляют в виде целого натурального числа разрядности n и сохраняют это число вместо результата деления в памяти для дальнейшего использования.

18. Способ по п. 14 или 16, отличающийся тем, что шифрование информации производят путем представления информации в 8-битных или соответственно 9-битных байтах, подстановки их в первую таблицу, сопоставления координат байтов исходной информации в первой таблице с аналогичными координатами байтов во второй таблице и замены байтов исходной информации на байты из второй таблицы с упомянутыми координатами и выводят полученные в результате замены байты криптограммы для последующей передачи, а дешифрование информации производят путем замены полученных байтов криптограммы на байты исходной информации путем подстановки их во вторую таблицу, сопоставления координат байтов криптограммы во второй таблице с аналогичными координатами байтов в первой таблице и замены байтов криптограммы на байты из первой таблицы с упомянутыми координатами и выводят полученные в результате замены байты

пользователю, при этом в случае шифрования и дешифрования электронных документов формирование новых таблиц производят с учётом заменяемых байтов электронных документов путём осуществления дополнительных операций с использованием тех ячеек, с помощью которых производилась замена байтов.

19. Система для осуществления криптозащитного сеанса связи, содержащая множество персональных криптозащитных комплексов, каждый из которых содержит

криптозащитное устройство, включающее в себя генератор случайных чисел, память для хранения материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), одинакового для всех криптозащитных устройств, память для хранения программ шифрования, дешифрования и обработки информации, и индивидуального номера криптозащитного устройства, связанные с памятью микропроцессор и средство защиты от несанкционированного доступа к материнскому коду и программам, порт ввода/вывода незашифрованной информации и порт ввода/вывода зашифрованной информации, связанные с памятью и микропроцессором,

терминал, включающий в себя порт ввода/вывода незашифрованной информации и порт ввода/вывода зашифрованной информации для подключения криптозащитного устройства, устройство ввода и устройство вывода, связанные с обоими портами ввода/вывода, по меньшей мере один порт для подключения к линии связи, соединенный с портом ввода/вывода зашифрованной информации.

20. Система по п. 19, отличающаяся тем, что терминал дополнительно содержит порт для подключения к соответствующему порту аналогичного терминала другого персонального криптозащитного комплекса.

21. Персональный криптозащитный комплекс для криптографической защиты конфиденциальной информации, проведения операций с соблюдением криптографических протоколов, финансовых операций и электронных сделок, содержащий

кассету, содержащую микросхему, включающую в себя микропроцессор, выполненный с возможностью подавления и маскирования собственных микроизлучений и создания ложных микроизлучений, энергонезависимую постоянную память для хранения программы шифрования, дешифрования и обработки информации и индивидуального номера кассеты, энергозависимую память для хранения материнского кода, содержащую встроенный аккумулятор, защитную оболочку микросхемы, снабженную блоком контроля целостности защитной оболочки, обеспечивающим стирание информации из энергозависимой памяти при несанкционированном внешнем доступе, порт ввода/вывода незашифрованной информации и порт ввода/вывода зашифрованной информации, связанные с микросхемой,

терминал, включающий в себя порт ввода/вывода незашифрованной информации и порт ввода/вывода зашифрованной информации для подключения кассеты, устройство ввода и

устройство вывода, связанные с обоими портами ввода/вывода, по меньшей мере один порт для подключения к линии связи, соединенный с портом ввода/вывода зашифрованной информации,

устройство для идентификации пользователя, выполненное в форме браслета, содержащее микросхему с памятью для хранения паролей доступа, идентифицирующих пользователя, порт для подключения к терминалу, причем браслет имеет датчики фиксации защелок для автоматического включения / выключения микросхемы для записи и удаления паролей доступа.

22. Кассета для персонального криптозащитного комплекса, предназначенная для защиты и хранения конфиденциальной и криптографической информации, содержащая

микросхему, включающую в себя микропроцессор, выполненный с возможностью подавления и маскирования собственных микроизлучений и создания ложных микроизлучений,

энергонезависимую постоянную память для хранения программ шифрования, дешифрования и обработки информации и индивидуального номера криптозащитного устройства,

энергозависимую память для хранения материнского кода, содержащую встроенный аккумулятор,

защитную оболочку микросхемы, соединённую с аккумулятором и блоком контроля целостности защитной оболочки, обеспечивающим стирание информации из энергозависимой памяти при несанкционированном внешнем доступе, и состоящую из трёх слоёв, из которых внутренний и внешний слои защитной оболочки выполнены со светоотражающими поверхностями, которые обращены друг к другу и между которыми размещен третий прозрачный слой, при этом на внутреннем светоотражающем слое расположены микро-светодиоды и микро-фотоэлементы, обращенные к внешнему светоотражающему слою, при этом блок контроля целостности защитной оболочки предназначен для задания и измерения периодичности и дозы излучения микро-светодиодов, измерения энергии, поглощаемой микро-фотоэлементами, сравнения измеренных значений с эталонными, и при их несовпадении-обесточивания энергозависимой памяти для уничтожения хранящегося в ней материнского кода.

23. Кассета по п. 22 отличающаяся тем, что микропроцессор содержит дополнительные параллельные дорожки для подачи сигналов, компенсирующих микроизлучения собственных сигналов микропроцессора, и генератор для формирования ложных микроизлучений в диапазоне частот собственных микроизлучений микропроцессора.

24. Способ защиты от навязывания ложной информации с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится

защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ индивидуальный номер I персонального криптозащитного комплекса,

формируют одноразовый ключ шифрования на основе по меньшей мере одного выработанного в упомянутом криптозащитном комплексе случайного числа,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования, причём динамически преобразуемый дочерний код предотвращает раскрытие кода пользователем, знающим исходную информацию и её зашифрованную криптограмму,

вводят исходную информацию, делят её на пакеты заранее определённого размера, шифруют каждый пакет информации для дальнейшей записи на носитель или передачи другому пользователю,

вводят или соответственно принимают зашифрованную информацию в персональный криптозащитный комплекс,

формируют одноразовый ключ дешифрования на основе упомянутого по меньшей одного случайного числа,

формируют динамически преобразуемый дочерний код на основе одноразового ключа дешифрования и материнского кода,

дешифруют принятую зашифрованную информацию, объединяют пакеты и выводят исходную информацию пользователю, причём подлинность источника шифрования информации устанавливают путём её дешифрования с помощью персонального криптозащитного комплекса, который дешифрует только ту информацию, которая зашифрована с применением аналогичного персонального криптозащитного комплекса с использованием общего материнского кода.

25. Способ защиты от навязывания ложной информации с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ индивидуальный номер I персонального криптозащитного комплекса,

формируют одноразовый ключ шифрования на основе по меньшей мере одного выработанного в упомянутом криптозащитном комплексе случайного числа,

формируют динамически преобразуемый дочерний код на основе материнского кода и одноразового ключа шифрования,

вводят исходную информацию, подвергают ее предварительной обработке для защиты от внесения изменений в зашифрованную информацию и установления тем самым подлинности исходной зашифрованной информации, шифруют предварительно обработанную информацию для дальнейшей записи на носитель или передачи другому пользователю,

вводят или соответственно принимают зашифрованную информацию в персональный криптозащитный комплекс,

формируют одноразовый ключ дешифрования на основе упомянутого по меньшей одного случайного числа,

формируют динамически преобразуемый дочерний код на основе одноразового ключа дешифрования и материнского кода,

дешифруют принятую зашифрованную информацию и устанавливают подлинность зашифрованной информации путем проверки того, что зашифрованная информация не была изменена, и только при положительном результате проверки дешифрованную информацию выводят пользователю.

26. Способ по п. 25, отличающийся тем, что предварительную обработку информации для защиты от внесения изменений в зашифрованную информацию осуществляют путем:

а) разделения исходной информации на пакеты,

б) хеширования каждого пакета исходной информации с помощью первой хеш-функции и добавления к пакету полученного первого результата хеширования,

в) шифрования каждого пакета, включая результат хеширования,

г) хеширования каждого зашифрованного пакета информации с помощью второй хеш-функции и добавления к зашифрованному пакету полученного второго результата хеширования для передачи зашифрованных пакетов и второго результата хеширования пользователю или для записи их на носитель,

а установление подлинности зашифрованной информации производят проверкой того, что зашифрованная информация не была изменена, осуществляют путем:

д) приема пользователем переданных зашифрованных пакетов и второго результата хеширования и восстановления частично потерянных или искаженных при передаче данных с использованием второго результата хеширования путем обратного хеширования с получением по меньшей мере одного варианта зашифрованного пакета информации,

е) дешифрования по меньшей мере одного варианта зашифрованного пакета информации и записи в оперативную память по меньшей мере одного дешифрованного пакета,

ж) обратного хеширования дешифрованных пакетов информации с использованием первого результата хеширования и поиск подлинного варианта исходной информации, причем только при нахождении упомянутого подлинного варианта он выводится пользователю, а все остальные дешифрованные пакеты удаляются из оперативной памяти.

27. Способ защиты от навязывания ложной информации с использованием персонального криптозащитного комплекса, включающий следующие этапы, осуществляемые в каждом из персональных криптозащитных комплексов:

а) в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

б) подключают по меньшей мере двух пользователей своими персональными криптозащитными комплексами к линии связи и установливают ими количество участников криптозащитного сеанса связи,

в) вырабатывают случайное число Z персональным криптозащитным комплексом и сохраняют его в оперативной памяти,

г) обмениваются по линии связи данными выработанных случайных чисел Z между упомянутыми персональными криптозащитными комплексами с установлением момента времени запуска формирования одноразового ключа сеанса связи,

д) синхронно формируют одноразовый ключ сеанса связи в персональных криптозащитных комплексах с использованием случайного числа, сохраненного в памяти, и случайного числа, полученного путем обмена данными по линии связи,

е) синхронно формируют динамически преобразуемый дочерний код в персональных криптозащитных комплексах на основе материнского кода и одноразового ключа сеанса связи,

ж) вводят и разделяют исходную передаваемую информацию на пакеты определенного размера и шифруют пакеты с использованием динамически преобразуемого дочернего кода,

з) передают зашифрованные пакеты информации по меньшей мере в один другой персональный криптозащитный комплекс,

и) принимают зашифрованные пакеты информации в упомянутом по меньшей мере одном другом персональном криптозащитном комплексе,

к) дешифруют принятые зашифрованные пакеты с использованием динамически преобразуемого дочернего кода,

л) объединяют дешифрованные пакеты в исходную информацию и выводят пользователю,

при этом повторяют этапы (е)-(л) для передачи информации в обратном направлении в том же сеансе связи, причём, защиту от навязывания ложной информации путём повторного использования зашифрованной и переданной ранее информации осуществляют используя одноразовые ключи сеанса связи формируемые в персональных криптозащитных комплексах на основе случайных чисел, одно из которых обязательно получают в каждом из персональных криптозащитных комплексов участников защищённой связи.

28. Способ защиты от навязывания ложной информации с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ персональные данные пользователя, включающих его электронную подпись, индивидуальный номер персонального криптозащитного комплекса и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

при введении пользовательской информации в персональный криптозащитный комплекс вводят команды пользователя для установки режима обработки пользовательской информации, формирования электронного документа и обрабатывают введенную пользовательскую информацию,

формируют с помощью программы обработки информации в соответствии с установленным режимом обработки пользовательской информации и ранее полученной информации служебную информацию, при этом вся служебная информация, вставляемая в электронный документ, является типовой, и объединяют ее с обработанной пользовательской информацией получая электронный документ, причем атрибуты электронного документа в виде служебной информации выделяют от обработанной пользовательской информации предварительно определенными в каждом персональном криптозащитном комплексе служебными символами, представляющими собой предварительно определённый набор битов, а в случае использования пользователем символов аналогичных служебным данные символы автоматически удаляют из пользовательской информации в процессе её обработки перед шифрованием, исключая тем самым навязывание ложной информации,

шифруют полученный в результате объединения электронный документ динамически преобразуемым дочерним кодом сформированным с применением по меньшей мере одного случайного числа и устанавливают защиту от внесения изменений в зашифрованную информацию,

вводят зашифрованную информацию в другой персональный криптозащитный комплекс и производят дешифрование, после чего устанавливают достоверность информации,

осуществляют поиск служебных символов и выделяют с их помощью служебную информацию находящуюся между служебных символов, вводят команды пользователя и устанавливают режим обработки дешифрованной информации в соответствии с командами пользователя, командами, полученными из служебной информации, ранее введённой информацией и программой обработки информации, и выводят обработанную информацию

пользователю вместе со служебными символами, которые выделяют и устанавливают подлинность атрибутов полученного электронного документа.

29. Способ по п. 28, отличающийся тем, что вводят команду пользователя на подписание электронного документа электронной цифровой подписью, состоящую из ранее введённых в ПЗУ персональных данных пользователя, индивидуального номера персонального криптозащитного комплекса, а также текущей даты и времени подписания электронного документа, и исходную информацию,

формируют пароль дешифрования электронного документа с применением по меньшей мере одного случайного числа и на его основе формируют одноразовый ключ шифрования данного электронного документа,

проверяют исходную информацию на отсутствие в ней символов, аналогичных служебным и в случае нахождения таковых удаляют из остальной исходной информации,

включают в состав введённого пользователем электронного документа информацию, считанную из ПЗУ, имеющую статус электронной цифровой подписи пользователя и выделяют её служебными символами,

делят полученную информацию на пакеты определённого размера, шифруют каждый пакет информации для дальнейшей записи на носитель или передачи другому пользователю,

вводят или соответственно принимают зашифрованную информацию в любой персональный криптозащитный комплекс,

формируют одноразовый ключ дешифрования на основе введённого пароля дешифрования данного электронного документа,

формируют динамически преобразуемый дочерний код на основе одноразового ключа дешифрования и материнского кода,

дешифруют принятую зашифрованную информацию, объединяют пакеты, выводят исходную информацию пользователю, выделяют из неё с помощью служебных символов электронную цифровую подпись и выводят пользователю на дисплей с указанием на то, что данная информация действительно является электронной цифровой подписью и именно данного электронного документа,

устанавливают с помощью электронной цифровой подписи дату и время подписания и лицо, подписавшее электронный документ, так как данные пользователя в электронной цифровой подписи предварительно заносятся регистратором в ПЗУ персонального криптозащитного комплекса одновременно с их регистрацией в общедоступной базе данных, а кроме того электронная цифровая подпись включает в себя электронную фотографию пользователя, которая позволяет идентифицировать электронную цифровую подпись без обращения к базе данных.

30. Способ по п. 29, отличающийся тем, что для регистрации электронной цифровой подписи пользователя берут данные пользователя, индивидуальный номер его персонального

криптозащитного комплекса, заявление пользователя записанное цифровой видеокамерой и содержащее информацию, позволяющую идентифицировать пользователя,

вводят информацию в персональный криптозащитный комплекс регистратора, подписывают полученную информацию электронной цифровой подписью регистратора, производят её шифрование и отправляют на центральный сервер,

вводят информацию в центральный криптозащитный комплекс, производят дешифрование полученной информации, заносят дешифрованную информацию в базу данных электронных цифровых подписей, формируют из полученной информации электронную цифровую подпись пользователя, заверяют её электронной цифровой подписью центрального криптозащитного комплекса содержащей заранее определённую информацию, шифруют и отправляют в персональный криптозащитный комплекс пользователя,

принимают и дешифруют информацию, в соответствии с заложенной программой проверяют электронную цифровую подпись пользователя на соответствие типовому шаблону, проверяют наличие электронной цифровой подписи центрального криптозащитного комплекса, сверяют индивидуальный номер, содержащийся в полученной электронной цифровой подписи пользователя с индивидуальным номером персонального криптозащитного номера пользователя и в случае положительных результатов записывают электронную цифровую подпись пользователя в ПЗУ его персонального криптозащитного комплекса.

31. Способ по п. 29, отличающийся тем, что электронные документы подписывают электронной цифровой подписью, имеющей статус электронной печати и содержащей данные определённого юридического лица, зарегистрированные в базе данных, причём данная электронная подпись содержится в ППЗУ персонального криптозащитного комплекса из которой может быть передана в ППЗУ другого персонального криптозащитного комплекса с одновременным автоматическим удалением из персонального криптозащитного комплекса, с которого произведена передача.

32. Способ передачи информации с защитой от копирования с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ, а также персональные данные пользователя, включающие его электронную подпись и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

при введении пользовательской информации в персональный криптозащитный комплекс вводят команды пользователя для установки режима обработки пользовательской информации,

формирования некопируемого электронного документа и обрабатывают введенную пользовательскую информацию,

формируют с помощью программы обработки информации в соответствии с установленным режимом обработки пользовательской информации и ранее полученной информации служебную информацию, объединяют ее с обработанной пользовательской информацией, получая электронный документ, причем атрибуты электронного документа в виде служебной информации отделяют от обработанной пользовательской информации предварительно определенными служебными символами, и в соответствии с командой пользователя - сформировать некопируемый электронный документ, включают в служебную информацию определённую команду для персональных криптозащитных комплексов в виде типового набора символов, заранее введённых в ПЗУ в составе программы обработки информации и сохраняют полученный электронный документ в отделе ППЗУ, предназначенном для некопируемых электронных документов, персонального криптозащитного комплекса,

устанавливают защищённый сеанс связи с применением персональных криптозащитных комплексов на основе одноразового ключа сеанса связи, сформированного с использованием случайных чисел и вводят команду пользователя передать записанный в ППЗУ некопируемый электронный документ другому абоненту установленного сеанса связи,

шифруют динамически преобразуемым дочерним кодом электронный документ, считывая при этом из служебной информации команду о некопируемости электронного документа, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в другой персональный криптозащитный комплекс,

в соответствии с командой о некопируемости по окончании передачи некопируемого электронного документа производят его блокирование на заранее определённый период времени Т1 в ППЗУ,

принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа, записывают электронный документ в отдел ППЗУ, предназначенный для не копируемых электронных документов и блокируют его на заранее определённый период времени Т1,

в персональном криптозащитном комплексе принимающей стороны формируют пароль подтверждения загрузки электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны,

в случае неполучения отправителем от получателя пароля подтверждения загрузки электронного документа в течение периода времени T1 производят разблокирование электронного документа в ППЗУ персонального криптозащитного комплекса отправителя, а последующее получение упомянутого пароля игнорируется,

в случае не отправления получателем отправителю пароля подтверждения загрузки электронного документа в течение периода времени T1 производят удаление электронного документа из ППЗУ персонального криптозащитного комплекса,

принимают пароль подтверждения загрузки электронного документа в персональном криптозащитном комплексе отправляющей стороны, формируют пароль подтверждения передачи электронного документа и запрашивают подтверждение пользователя на отправление данного пароля в персональный криптозащитный комплекс принимающей стороны,

в случае, если пользователь не даёт подтверждение на отправление пароля в течение заранее определённого периода времени T2, то по истечении данного периода времени в ППЗУ персонального криптозащитного комплекса отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ персонального криптозащитного комплекса получателя упомянутый электронный документ автоматически удаляют,

в случае, если пользователь даёт подтверждение на отправление пароля в течение периода времени T2, то данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс получателя, при этом упомянутый электронный документ автоматически удаляют из ППЗУ персонального криптозащитного комплекса отправителя, а в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа автоматически производят разблокирование упомянутого электронного документа, после чего вводят команды пользователя, устанавливают режим обработки дешифрованной информации в соответствии с командами пользователя, командами, полученными из служебной информации, ранее введённой информацией и программой обработки информации и выводят обработанную информацию пользователю вместе со служебными символами, которые устанавливают подлинность атрибутов полученного электронного документа.

33. Способ по п. 32, отличающийся тем, что в персональный криптозащитный комплекс получают зашифрованную информацию, являющуюся не копируемым электронным документом, содержащим переменный номинал, обозначенный предварительно определённым образом с помощью служебных символов,

дешифруют информацию и записывают полученный электронный документ в ППЗУ персонального криптозащитного комплекса,

с помощью программы обработки информации определяют служебные символы в электронном документе,

определяют служебную информацию, обозначенную служебными символами,

определяют в служебной информации информацию о переменном номинале электронного документа и выводят данную информацию пользователю,

дробят электронный документ на произвольные части, изменяя с помощью программы обработки информации номиналы частей таким образом, что их общая сумма, остаётся неизменной, при этом остальные характеристики и атрибуты частей электронного документа также остаются неизменяемыми,

отправляют части электронного документа в другие персональные криптозащитные комплексы,

принимают в персональный криптозащитный комплекс несколько одинаковых электронных документов с переменным номиналом и автоматически с помощью программы обработки информации собирают в единый электронный документ, суммируя их номиналы.

34. Способ по п. 33 отличается тем, что электронным документом с переменным номиналом является электронный переводной банковский вексель с заранее определённым сроком погашения, содержащий в служебной информации электронного документа данные банка, выдавшего вексель, включая электронные цифровые подписи банка, сформированные с помощью персонального криптозащитного комплекса, данные пользователя, которому выдан вексель, валюту и номинал векселя, а также дату погашения векселя, после которой в банке произведут разблокирование оставшейся на счету пользователя залоговой суммы денег, которые досрочно передадут любому предъявителю данного электронного векселя либо его части, после того как примут электронный вексель в персональный криптозащитный комплекс банка, идентифицируют данные электронного векселя, определят его номинал и в случае, если указанная в электронном векселе дата погашения не превышает текущей даты, выдадут предъявителю сумму, соответствующую номиналу предъявленного электронного векселя.

35. Способ передачи информации с защитой от копирования с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ индивидуальный номер персонального криптозащитного комплекса, а также другие атрибуты, которые используются для совершения криптозащитных операций и устанавливают дату и время во встроенных часах,

формируют пароль дешифрования на основе случайного числа и записывают его в отдел ППЗУ, предназначенный для некопируемых паролей дешифрования и закрытый для пользователей,

формируют динамически преобразуемый дочерний код на основе материнского кода и пароля дешифрования ,

вводят в персональный криптозащитный комплекс информацию, в том числе компьютерную программу, и производят её шифрование с использованием упомянутого пароля дешифрования,

выводят зашифрованную информацию пользователю для записи на носитель или для передачи другому пользователю,

вводят команду передать пароль дешифрования другому пользователю в процессе защищённого сеанса связи,

шифруют пароль дешифрования на основе одноразового ключа, сформированного с использованием по меньшей мере одного случайного числа и выводят его для передачи,

в соответствии с тем, что пароль дешифрования имеет статус некопируемого электронного документа, то по окончанию передачи данного электронного документа производят его блокирование на заранее определённый период времени Т1 в ППЗУ,

принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят с помощью служебных символов служебную информацию, содержащую команду о не копируемости электронного документа, записывают электронный документ в отдел ППЗУ, предназначенный для не копируемых электронных документов и блокируют его на заранее определённый период времени Т2,

в персональном криптозащитном комплексе принимающей стороны формируют пароль подтверждения загрузки электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны,

в случае неполучения отправителем от получателя пароля подтверждения загрузки электронного документа в течение периода времени Т1 производят разблокирование электронного документа в ППЗУ персонального криптозащитного комплекса отправителя, и игнорируют последующее получение упомянутого пароля,

в случае не отправления получателем отправителю пароля подтверждения загрузки электронного документа в течение периода времени Т1, производят удаление электронного документа из ППЗУ персонального криптозащитного комплекса,

принимают пароль подтверждения загрузки электронного документа в персональном криптозащитном комплексе отправляющей стороны, формируют пароль подтверждения передачи электронного документа и запрашивают подтверждение пользователя на отправление данного пароля в персональный криптозащитный комплекс принимающей стороны,

в случае, если пользователь не даёт подтверждение на отправление пароля в течение периода времени Т2, то по истечению данного периода времени в ППЗУ персонального криптозащитного комплекса отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ персонального криптозащитного комплекса получателя упомянутый электронный документ автоматически удаляют,

в случае, если пользователь даёт подтверждение на отправление пароля в течение периода времени Т2, то данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс получателя, при этом упомянутый электронный документ автоматически удаляют из ППЗУ персонального криптозащитного комплекса отправителя, а в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа автоматически производят разблокирование упомянутого электронного документа,

после чего записывают пароль дешифрования в отдел ППЗУ персонального криптозащитного комплекса, предназначенный для некопируемых паролей дешифрования и закрытый для пользователей ППЗУ,

вводят в персональный криптозащитный комплекс информацию, в том числе компьютерную программу и производят дешифрование на основе динамически преобразуемого кода, сформированного с помощью считанного из ППЗУ пароля дешифрования,

в случае с дешифрованием компьютерной программы подключают персональный криптозащитный комплекс к компьютеру, записывают дешифрованный фрагмент программы в ОЗУ персонального криптозащитного комплекса, выполняют одну часть операций в микропроцессоре персонального криптозащитного комплекса, совместимого с компьютером, а другую в микропроцессоре компьютера.

36. Способ по п. 35, отличающийся тем, что дополнительно вводят команду пользователя на ограничение периода действия пароля дешифрования по времени или по количеству раз использования,

включают в пароль дешифрования соответствующие служебные команды и выделяют их служебными символами,

шифруют полученные служебные команды в составе пароля дешифрования и выводят для дальнейшей записи на носитель или передачи другому пользователю, сохраняя при этом пароль дешифрования в ППЗУ,

одновременно блокируют доступ к паролю дешифрования, оставшемуся в ППЗУ персонального криптозащитного комплекса пользователя на заранее определённый промежуток времени,

вводят или соответственно принимают зашифрованный пароль дешифрования, с включёнными в него служебными командами,

выделяют с помощью служебных символов служебные команды и производят операции с данным паролем дешифрования в соответствии с полученными командами из служебной информации, а именно, удаляют из памяти персонального криптозащитного комплекса пароль дешифрования по истечении указанного в служебной информации времени или после использования пароля дешифрования указанное в служебной информации количество раз.

37. Способ по п. 35, отличающийся тем, что вводят команду передать пароль дешифрования другому пользователю в зашифрованном электронном письме,

добавляют к паролю дешифрования служебную информацию, выделенную служебными символами, с указанием индивидуального номера персонального криптозащитного комплекса получателя, а также даты и времени, по истечении которых получатель данного пароля дешифрования сможет передать его другим пользователям криптозащитных персональных комплексов,

одновременно в персональном криптозащитном комплексе отправителя пароля дешифрования формируют электронное письмо, в которое включают пароль дешифрования с добавленной к нему служебной информацией, а также дополнительно указывают дату и время в виде служебной информации, только до истечения которых персональный криптозащитный комплекс получателя электронного письма сможет расшифровать данное сообщение, причём, дату и время дешифрования электронного письма указывают меньшую или аналогичную дате и времени, указанных в служебной информации пароля дешифрования,

шифруют сформированное электронное письмо динамически преобразуемым кодом на основе одноразового ключа, формируемого из случайного числа и индивидуального номера персонального криптозащитного комплекса получателя данного электронного письма и добавляют к зашифрованному электронному письму упомянутое случайное,

выводят зашифрованное электронное письмо и случайное число для передачи адресату вместе с зашифрованной с помощью пароля дешифрования информацией,

записывают зашифрованное электронное письмо, содержащее пароль дешифрования, вместе со случайным числом на носитель или передают по линии связи и по окончании передачи удаляют пароль дешифрования из ППЗУ персонального криптозащитного комплекса отправителя,

принимают зашифрованное электронное письмо, случайное число и зашифрованную информацию,

вводят случайное число в ОЗУ персонального криптозащитного комплекса и считывают индивидуальный номер персонального криптозащитного комплекса из ПЗУ, также записывая его в ОЗУ,

формируют одноразовый ключ на основе введённого случайного числа и считанного индивидуального номера,

формируют динамически преобразуемый код на основе одноразового ключа и вводят в персональный криптозащитный комплекс зашифрованное электронное письмо,

производят дешифрование электронного письма с помощью динамически преобразуемого кода и записывают в ОЗУ дешифрованный текст электронного письма,

определяют служебную информацию с помощью служебных символов, находят служебную информацию с указанием окончательных даты и времени дешифрования электронного письма и сверяются с датой и временем во встроенных часах и в случае превышения указанных даты и времени над текущими производят удаление данного электронного письма из ОЗУ,

находят пароль дешифрования, включающий дату и время, по истечении которых может быть произведена передача пароля дешифрования другим пользователям, и записывают в отдел ППЗУ персонального криптозащитного комплекса, предназначенный для не копируемых паролей дешифрования и закрытый для пользователей ППЗУ,

вводят в персональный криптозащитный комплекс информацию, в том числе компьютерную программу и производят дешифрование на основе динамически преобразуемого кода, сформированного с помощью считанного из ППЗУ пароля дешифрования,

по истечении даты и времени, указанных в служебной информации, включённой в пароль дешифрования, удаляют из ППЗУ данную служебную информацию, одновременно снимая ограничение на дальнейшую передачу пароля дешифрования другим пользователям.

38. Способ по п. 32 или 35, отличающийся тем, что к передаваемому электронному документу добавляют временный индивидуальный номер, формируемый генератором случайных чисел, и произвольно вводимое значение периода времени Т2, которые шифруют вместе с электронным документом,

вводят команду передать электронный документ другому пользователю в процессе защищённого сеанса связи или в зашифрованном электронном письме,

по окончанию передачи данного электронного документа производят его блокирование на заранее определённый период времени Т1 в ППЗУ отправителя и отмечают его присвоенным временным индивидуальным номером,

в случае сбоев при передаче электронного документа отправитель осуществляет повторное отправление данного электронного документа с теми же сопутствующими данными,

принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят с помощью служебных символов служебную информацию, содержащую команду о не копируемости электронного документа и

временный индивидуальный номер данного документа, сверяют данный номер на наличие в ППЗУ заблокированного электронного документа с таким же номером и в случае отсутствия совпадения записывают электронный документ в отдел ППЗУ, предназначенный для не копируемых электронных документов, отмечают его присвоенным временным индивидуальным номером и блокируют электронный документ на заранее определённый период времени T1,

в персональном криптозащитном комплексе принимающей стороны на основе случайного числа формируют пароль подтверждения загрузки электронного документа, автоматически добавляют к нему упомянутый временный индивидуальный номер данного электронного документа, записывают копию пароля в ППЗУ и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны в процессе защищённого сеанса связи или в зашифрованном электронном письме,

принимают пароль подтверждения загрузки электронного документа в персональном криптозащитном комплексе отправляющей стороны, находят в ППЗУ заблокированный электронный документ, отмеченный номером, соответствующим номеру, полученному с паролем, и в случае наличия заблокированного электронного документа и совпадения номеров формируют пароль подтверждения передачи электронного документа с использованием пароля подтверждения загрузки электронного документа, автоматически включая в него упомянутый временный индивидуальный номер электронного документа,

запрашивают подтверждение пользователя на отправление данного пароля в персональный криптозащитный комплекс принимающей стороны,

в случае, если пользователь не даёт подтверждение на отправление пароля в течение произвольного периода времени T2, значение которого заранее вводится отправителем при установлении режима отправления электронного документа, то по истечении данного периода времени в ППЗУ персонального криптозащитного комплекса отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ персонального криптозащитного комплекса получателя упомянутый электронный документ автоматически удаляют,

в случае, если пользователь даёт подтверждение на отправление пароля в течение периода времени T2, то данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс получателя, при этом упомянутый электронный документ автоматически удаляют из ППЗУ персонального криптозащитного комплекса отправителя, а в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа находят в ППЗУ заблокированный электронный документ и записанную копию пароля подтверждения загрузки электронного документа, отмеченные номером, соответствующим номеру, полученному с паролем, и только в случае наличия заблокированного электронного документа, совпадения номеров и наличия

прямой связи между паролями автоматически производят разблокирование упомянутого электронного документа,

после чего записывают электронный документ в отдел ППЗУ персонального криптозащитного комплекса, предназначенный для некопируемых электронных документов и закрытый для пользователей ППЗУ, и удаляют упомянутый временный индивидуальный номер,

в случае сбоев при передаче электронного документа или паролей подтверждения пользователи осуществляют дублирование передачи.

39. Способ по п. 38, отличающийся тем, что к передаваемому электронному документу добавляют индивидуальный номер N1 персонального криптозащитного комплекса, с которого будут осуществлять отправление пароля подтверждения передачи электронного документа, временный индивидуальный номер N2, формируемый генератором случайных чисел и бесконечное значение периода времени T2 , вводимое пользователем, которые шифруют вместе с электронным документом,

вводят команду передать электронный документ другому пользователю в процессе защищённого сеанса связи,

по окончании передачи данного электронного документа производят его блокирование на заранее определённый период времени T1 в ППЗУ отправителя и отмечают его присвоенным упомянутым номером N2,

принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа и номера данного документа, записывают электронный документ в отдел ППЗУ, предназначенный для некопируемых электронных документов, отмечают его присвоенным номером N2 и блокируют электронный документ на заранее определённый период времени T1,

в персональном криптозащитном комплексе принимающей стороны формируют пароль подтверждения загрузки электронного документа, автоматически добавляют к нему упомянутый номер N2 данного электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны в процессе того же или другого защищённого сеанса связи,

принимают пароль подтверждения загрузки электронного документа в персональном криптозащитном комплексе отправляющей стороны, находят в ППЗУ заблокированный электронный документ, отмеченный номером N2, соответствующим номеру, полученному с

паролем и в случае наличия заблокированного электронного документа и совпадения номеров удаляют из ППЗУ данный электронный документ, так как период времени Т2 равен бесконечному значению,

в персональном криптозащитном комплексе, индивидуальный номер которого соответствует номеру N1, присвоенному электронному документу, вводят числовое значение соответствующее номеру N2 электронного документа, формируют пароль подтверждения передачи электронного документа, автоматически включая в него свой индивидуальный номер соответствующий N1, и введённый номер N2,

данный пароль в зашифрованном виде отправляют в персональный криптозащитный комплекс получателя электронного документа,

в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа находят в ППЗУ заблокированный электронный документ, отмеченный номером N2, соответствующим номеру, полученному с паролем, сверяют номера N1, находящиеся в электронном документе и в пароле, и только в случае совпадения номеров автоматически производят разблокирование упомянутого электронного документа,

после чего записывают электронный документ в отдел ППЗУ персонального криптозащитного комплекса, предназначенный для некопируемых электронных документов, и удаляют добавленные номера N1 и N2.

40. Способ по п. 38 отличающийся тем, что к передаваемому электронному документу добавляют временный индивидуальный номер, формируемый генератором случайных чисел, и вводят бесконечное значение периода времени Т2, которые шифруют вместе с электронным документом,

вводят команду сформировать пароль подтверждения передачи данного электронного документа,

формируют пароль подтверждения электронного документа, присваивают ему номер и, при наличии, переменный номинал, соответствующие временному номеру и переменному номиналу электронного документа,

передают пароль подтверждения электронного документа в процессе криптозащитного сеанса связи в зашифрованном виде определённому пользователю либо оставляют в своём персональном криптозащитном комплексе,

блокируют электронный документ в ППЗУ персонального криптозащитного комплекса на произвольный период времени Т1, делают копии с электронного документа с соответствующей об этом пометкой и передают копии другим пользователям в процессе защищённого сеанса связи или в зашифрованном электронном письме,

по окончании периода времени Т1 удаляют электронный документ из ППЗУ отправителя,

принимают копии электронного документа, производят дешифрование электронного документа, осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят пометку о том, что это копия электронного документа, временный индивидуальный номер данного документа, записывают электронный документ в ППЗУ и отмечают его присвоенным временным индивидуальным номером,

в персональный криптозащитный комплекс одного из пользователей, принявших копию электронного документа принимают пароль подтверждения передачи электронного документа, находят в ППЗУ копию электронного документа, отмеченную номером, соответствующим номеру, полученному с паролем, и в случае совпадения номеров снимают с копии электронного документа пометку о том, что это копия электронного документа, после чего записывают электронный документ в отдел ППЗУ персонального криптозащитного комплекса, предназначенный для некопируемых электронных документов и закрытый для пользователей ППЗУ, и удаляют упомянутый временный индивидуальный номер,

в персональном криптозащитном комплексе отправителя пароля подтверждения передачи электронного документа после осуществления передачи данного пароля автоматически производят его удаление из ППЗУ, а в случае передачи части пароля с переменным номиналом в оставшейся в ППЗУ части пароля уменьшают его номинал на сумму, равную переданной части.

41. Способ идентификации пользователя с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ персональные данные пользователя, включающие его электронную подпись, индивидуальный номер персонального криптозащитного комплекса и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

при введении пользовательской информации в персональный криптозащитный комплекс вводят команды пользователя для установки режима обработки пользовательской информации, формирования электронного документа и совершения криптозащитной операции,

перед совершением криптозащитных операций подключают к персональному криптозащитному комплексу средство идентификации пользователя, в памяти которого на момент подключения отсутствует идентифицирующая пользователя информация,

выдают пользователю запрос об идентификации пользователя,

вводят пользователем через средство ввода информации идентификационные данные пользователя и сверяют их с хранимыми в памяти криптозащитного комплекса идентификационными данными, предварительно введёнными пользователем,

в случае совпадения введённых пользователем идентификационных данных со считанными из памяти вырабатывают генератором случайных чисел одноразовые пароли доступа и сохраняют их одновременно в персональном криптозащитном комплексе и средстве идентификации пользователя, выполненном с возможностью удаления из памяти хранимых одноразовых паролей доступа,

непосредственно перед совершением криптозащитной операции, требующей проведения идентификации пользователя, выдают пользователю запрос об идентификации пользователя,

осуществляют подключение средства идентификации пользователя к персональному криптозащитному комплексу и производят передачу одноразового пароля доступа из средства идентификации пользователя в персональный криптозащитный комплекс с одновременным удалением использованного одноразового пароля из памяти средства идентификации,

сравнивают полученный одноразовый пароль доступа с хранимым в памяти персонального криптозащитного комплекса одноразовым паролем, и в случае совпадения паролей совершают криптозащитную операцию,

42. Способ по п. 41, отличающийся тем, что пользователь идентифицирует себя с помощью средства идентификации для доступа к определённым объектам, содержащим электронные замки, в которых заранее сохраняют одноразовые пароли доступа, одновременно сохраняемые в персональном криптозащитном комплексе и в средстве идентификации пользователя, выполненном с возможностью быстрого удаления из памяти хранимых одноразовых паролей, а идентификация пользователя производится путём сравнения получённого из средства идентификации одноразового пароля доступа с хранимым в памяти объекта доступа одноразовым паролем, и в случае совпадения паролей производят доступ пользователя к объекту, причём одноразовые пароли доступа могут быть получены генераторами псевдослучайных чисел, находящимися в персональном криптозащитном комплексе пользователя и в электронном замке объекта доступа, работающими по аналогичной программе и вырабатывающими одинаковые одноразовые пароли доступа .

43. Устройство для идентификации пользователя, выполненное в форме браслета, надеваемого на запястье пользователя, содержащее микросхему с памятью для хранения одноразовых паролей доступа, идентифицирующих пользователя, поводок с портом для подключения к персональному криптозащитному комплексу и объектам доступа, датчики фиксации защелок браслета для автоматического включения/выключения микросхемы для записи одноразовых паролей доступа и их автоматического удаления при снятии браслета.

44. Устройство по п. 43, отличающийся тем, что браслет содержит беспроводный интерфейс для сопряжения с каналом беспроводной передачи данных.

45. Устройство по п. 43, отличающийся тем, что поводок, предназначенный для подключения браслета к персональному криптозащитному комплексу, одновременно служит для снабжения энергией аккумулятора браслета.

46. Устройство по п. 43, отличающийся тем, что браслет снабжён устройством для автоматической замены аккумуляторов при подключении к терминалу.

47. Способ одновременного обмена электронными документами, защищёнными от копирования, между пользователями по линии связи с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ индивидуальный номер I персонального криптозащитного комплекса, а также персональные данные пользователя, включающие его электронную подпись и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

синхронно формируют одноразовый ключ шифрования на основе выработанных в персональных криптозащитных комплексах пользователей случайных числах,

синхронно формируют динамически преобразуемые дочерние коды на основе материнского кода и одноразового ключа шифрования в персональных криптозащитных комплексах пользователей,

вводят исходную информацию в каждый из персональных криптозащитных комплексов пользователей, формируют с помощью программы обработки информации в соответствии с установленным режимом обработки пользовательской информации и ранее полученной информации служебную информацию, объединяют ее с обработанной пользовательской информацией, получая электронный документ, причем атрибуты электронного документа в виде служебной информации отделяют от обработанной пользовательской информации предварительно определенными служебными символами, и в соответствии с командой пользователя - сформировать электронный документ, защищённый от копирования, включают в служебную информацию определённую команду для персональных криптозащитных комплексов в виде типового набора символов, заранее введённых в ПЗУ в составе программы обработки информации, и сохраняют полученный электронный документ в отделе ППЗУ, предназначенном для не копируемых электронных документов, персонального криптозащитного комплекса,

по меньшей мере в одном из персональных криптозащитных комплексов вводят команду одновременного обмена электронными документами и посылают данную команду в

виде зашифрованного с помощью выработанного одноразового ключа шифрования сигнала в другой персональный криптозащитный комплекс,

в каждом из персональных криптозащитных комплексов вводят команду пользователя начать передачу записанного в ППЗУ некопируемого электронного документа другому абоненту установленного сеанса связи,

шифруют динамически преобразуемым дочерним кодом электронный документ, считывая при этом из служебной информации команду о некопируемости электронного документа, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в другой персональный криптозащитный комплекс,

в соответствии с командой об одновременном обмене электронных документов по окончанию передачи некопируемого электронного документа производят его блокирование на заранее определённый период времени T1 в ППЗУ отправителя,

принимают электронный документ и производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации,

осуществляют поиск и выделение служебной информации из дешифрованной информации с помощью служебных символов, находят с помощью служебных символов служебную информацию, содержащую команду о некопируемости электронного документа, записывают электронный документ в отдел ППЗУ, предназначенный для некопируемых электронных документов, блокируют его на заранее определённый период времени T1 и выводят полученный электронный документ пользователю для ознакомления,

в персональном криптозащитном комплексе принимающей стороны формируют пароль подтверждения загрузки электронного документа и в зашифрованном виде передают пароль подтверждения загрузки электронного документа в персональный криптозащитный комплекс отправляющей стороны,

в случае неполучения отправителем от получателя пароля подтверждения загрузки электронного документа в течение периода времени T1 производят разблокирование электронного документа в ППЗУ персонального криптозащитного комплекса отправителя,

в случае неотправления получателем отправителю пароля подтверждения загрузки электронного документа в течение периода времени T1 производят удаление электронного документа из ППЗУ персонального криптозащитного комплекса получателя,

принимают пароль подтверждения загрузки электронного документа в персональном криптозащитном комплексе отправляющей стороны, формируют пароль подтверждения передачи электронного документа и запрашивают подтверждение пользователя на отправление данного пароля в персональный криптозащитный комплекс принимающей стороны,

в случае, если пользователь не даёт подтверждение на отправление пароля в течение заранее определённого периода времени T2, то по истечении данного периода времени в ППЗУ

персонального криптозащитного комплекса отправителя производят автоматическое разблокирование упомянутого электронного документа, а в ППЗУ персонального криптозащитного комплекса получателя упомянутый электронный документ автоматически удаляют,

в случае, если пользователь даёт подтверждение на отправление пароля в течение периода времени Т2, то отправляют другому пользователю в зашифрованном виде заранее определённый сигнал, содержащий информацию о данном подтверждении и получают аналогичный сигнал от упомянутого пользователя,

после обмена подтверждающими сигналами производят синхронизацию по последнему сигналу и с момента отправления в одном из персональных криптозащитных комплексов и соответственно получения в другом персональном криптозащитном комплексе последнего бита упомянутого сигнала начинают процедуру одновременного обмена в зашифрованном виде паролями подтверждения передачи электронного документа, причём в каждом из персональных криптозащитных комплексов контролируют получение сигнала, содержащего пароль от противоположной стороны, и в случае отсутствия или прерывания данного сигнала прекращают передачу своего пароля,

после отправления пароля подтверждения передачи упомянутый электронный документ автоматически удаляют из ППЗУ персонального криптозащитного комплекса отправителя, а в ППЗУ персонального криптозащитного комплекса получателя после получения им пароля подтверждения передачи электронного документа автоматически производят разблокирование упомянутого электронного документа.

48. Способ по п. 47, отличающийся тем, что в последний подтверждающий сигнал автоматически вводят значение времени Т, отличающееся от текущего показания времени на период времени t, значение которого формируется с помощью генератора случайных чисел,

отправляют данный сигнал другому пользователю и по истечении отправления сигнала до наступления времени Т передают случайный сигнал, формируемый генератором случайных чисел,

при наступлении времени Т автоматически прекращают передачу случайного сигнала и начинают одновременную передачу в зашифрованном виде паролей подтверждения передачи электронных документов, причём случайный сигнал и криптограмма паролей имеют одинаковые характеристики.

49. Способ по п. 47, отличающийся тем, что пользователи обмениваются копией электронного документа, которую предварительно подписывают каждый своей электронной цифровой подписью, и после получения, блокирования в ППЗУ и ознакомления с полученными электронными документами, по меньшей мере одним из пользователей вводится команда одновременного подписания данного электронного документа,

посылается сигнал в зашифрованном виде другому пользователю, содержащий информацию об одновременном подписании электронного документа и выводится пользователю,

после обмена паролями подтверждения передачи электронных документов в каждом из персональных криптозащитных комплексов автоматически производят подписание полученных электронных документов электронной цифровой подписью пользователя.

50. Способ по п. 47, отличающийся тем, что в одном из персональных криптозащитных комплексов вводят команду отправить электронное письмо с уведомлением, вводят информацию, добавляют к данной информации номер, сформированный генератором случайных чисел, выделяют его заранее введёнными служебными символами и шифруют информацию с номером с применением пароля дешифрования,

в соответствии с упомянутой командой записывают пароль дешифрования в ППЗУ персонального криптозащитного комплекса и отмечают его упомянутым номером,

формируют электронное письмо с уведомлением из введённой зашифрованной информации и добавленной к ней служебной информации, отделённой заранее введёнными служебными символами, в которой содержится номер, соответствующий номеру информации, и пароль дешифрования, и введена команда о том, что данная информация является электронным письмом с уведомлением, копию зашифрованного электронного письма с уведомлением выводят для записи на носитель,

устанавливают криптозащитный сеанс связи с определённым пользователем с применением персональных криптозащитных комплексов и передают электронное письмо с уведомлением,

принимают информацию, дешифруют служебную информацию, находят номер, который записывают в ППЗУ, команду о том, что полученная зашифрованная информация является электронным письмом с уведомлением, и выводят данную команду пользователю,

в соответствии с упомянутой командой и вводимой получателем командой – отправить уведомление о получении данного сообщения отправителю, формируют электронный документ в виде заранее введённого типового бланка уведомления, вводят в него номер, соответствующий номеру полученной информации, и подписывают данный электронный документ электронной подписью пользователя, содержащей текущие дату и время,

отправляют другому пользователю в зашифрованном виде заранее определённый сигнал, содержащий информацию, подтверждающую наличие уведомления,

после отправления и соответственно получения упомянутого сигнала производят одновременный обмен электронного бланка уведомления на пароль дешифрования электронного письма,

принимают пароль дешифрования в персональный криптозащитный комплекс получателя, с его помощью расшифровывают информацию, полученную в электронном письме с уведомлением, и выводят пользователю,

принимают электронный документ, являющийся бланком уведомления о получении электронного письма с уведомлением, в персональный криптозащитный комплекс отправителя, расшифровывают его и выводят пользователю, а криптограмму бланка уведомления записывают на носитель.

51. Способ по п. 50, отличающийся тем, что в персональном криптозащитном комплексе отправителя вводят команду отправить электронное письмо с уведомлением, вводят информацию, добавляют к данной информации номер N, сформированный генератором случайных чисел, выделяют его заранее введёнными служебными символами, вводят индивидуальный номер I персонального криптозащитного комплекса адресата, генерируют случайное число Z,

на основе введённого номера I и случайного числа Z формируют одноразовый ключ шифрования и шифруют информацию, включая добавленный случайный номер N,

в соответствии с упомянутой командой записывают случайное число Z в ППЗУ персонального криптозащитного комплекса и отмечают его упомянутым случайным номером N,

формируют электронное письмо с уведомлением из введённой зашифрованной информации и добавленной к ней служебной информации, отделённой заранее введёнными служебными символами, в которой содержится номер, соответствующий номеру N информации, и введена команда о том, что данная информация является электронным письмом с уведомлением, копию зашифрованного электронного письма с уведомлением выводят для записи на носитель,

передают электронное письмо с уведомлением в узловой компьютер, устанавливают криптозащитный сеанс связи с узловым криптозащитным комплексом, подключенным к узловому компьютеру, передают случайное число Z, которое сохраняют в узловом криптозащитном комплексе,

принимают электронное письмо с уведомлением с узлового компьютера в персональный криптозащитный комплекс адресата, дешифруют служебную информацию, находят номер N, который записывают в ППЗУ, команду о том, что полученная зашифрованная информация является электронным письмом с уведомлением, и выводят данную команду пользователю,

в соответствии с упомянутой командой и вводимой получателем командой – отправить уведомление о получении данного сообщения отправителю, формируют электронный документ в виде заранее введённого типового бланка уведомления, вводят в него номер N, соответствующий номеру полученной информации, и подписывают данный электронный документ электронной подписью пользователя, содержащей текущие дату и время,

отправляют в узловой криптозащитный комплекс через узловой компьютер в зашифрованном виде заранее определённый сигнал, содержащий информацию, подтверждающую наличие уведомления,

после отправления и соответственно получения упомянутого сигнала производят одновременный обмен электронного бланка уведомления на случайное число Z,

принимают случайное число Z в персональный криптозащитный комплекс получателя, выводят из ПЗУ индивидуальный номер I персонального криптозащитного комплекса и на их основе формируют одноразовый ключ дешифрования,

расшифровывают информацию, полученную в электронном письме с уведомлением, и выводят пользователю,

в персональный криптозащитный комплекс отправителя принимают с узлового криптозащитного комплекса через узловой компьютер электронный документ, являющийся бланком уведомления о получении электронного письма с уведомлением, в персональный криптозащитный комплекс отправителя, расшифровывают его и выводят пользователю, а криптограмму бланка уведомления записывают на носитель.

52. Способ конвертации электронных наличных денег или бессрочных электронных векселей в электронные деньги несовместимых платёжных систем с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ персональные данные пользователя, включающие его электронную подпись и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

с помощью заранее заложенной программы в персональном криптозащитном комплексе банка формируют электронный документ, с применением заранее определённых служебных символов, предназначенный для определённого пользователя, в который включают подписанную банком электронную банкноту, условия банка в виде определённых команд,

устанавливают криптозащитный сеанс связи с применением персональных криптозащитных комплексов между банком и пользователем, и передают пользователю сформированный электронный документ,

принимают в персональный криптозащитный комплекс пользователя упомянутый электронный документ, расшифровывают, определяют служебные символы, с их помощью определяют команды и электронную банкноту, подписанную банком, записывают электронную

банкноту в ППЗУ персонального криптозащитного комплекса и блокируют до получения определённых команд и выполнения условий банка, содержащихся в полученных командах электронного документа,

принимают в персональный криптозащитный комплекс пользователя электронные наличные деньги или электронные банковские векселя, вводят команду пользователя разблокировать электронную банкноту, подписанную банком,

в соответствии с командой пользователя проверяют наличие в ППЗУ электронных наличных денег или электронных банковских векселей и их соответствие условиям банка по сумме, валюте и другим атрибутам,

при выполнении условий банка производят блокирование определённой данным условием суммы электронных наличных денег или электронных банковских векселей и одновременное разблокирование электронной банкноты, причём сумма блокируемых электронных наличных денег или векселей в соответствии с условиями банка может превышать сумму электронной банкноты,

подключают к персональному криптозащитному комплексу пользователя посредством терминала носитель и производят передачу электронной банкноты на данный носитель,

производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя,

в банке принимают данную электронную банкноту, заносят её в регистр, и если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя,

выставляют на банковский счёт пользователя счёт на сумму потраченной электронной банкноты за вычетом сдачи с момента проведения транзакции платежа и одновременно вводят информацию о сумме кредита в персональный криптозащитный комплекс банка в виде заранее определённых команд,

подключают персональный криптозащитный комплекс пользователя к персональному криптозащитному комплексу банка, устанавливают между ними криптозащитный сеанс связи, идентифицируют персональные криптозащитные комплексы и вводят команду на погашение кредита,

производят расчёт суммы для разблокирования в соответствии с суммой и сроком кредита, разблокируют определённую расчётом сумму электронных наличных денег или электронных банковских векселей, необходимую для погашения кредита сумму передают в персональный криптозащитный комплекс банка, а оставшаяся часть разблокированной суммы остаётся в распоряжении пользователя.

53. Способ конвертации электронных банковских векселей в электронные деньги несовместимых платёжных систем с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

сохраняют в ПЗУ индивидуальный номер персонального криптозащитного комплекса, а также персональные данные пользователя, включающие его электронную подпись и другие атрибуты, которые используются для совершения криптозащитных операций и формирования электронных документов, и устанавливают дату и время во встроенных часах,

с помощью заранее заложенной программы в персональном криптозащитном комплексе банка формируют электронный документ, с применением заранее определённых служебных символов, предназначенный для определённого пользователя, в который включают подписанную банком электронную банкноту, условия банка в виде определённых команд,

устанавливают криптозащитный сеанс связи с применением персональных криптозащитных комплексов между банком и пользователем, и передают пользователю сформированный электронный документ,

принимают в персональный криптозащитный комплекс пользователя упомянутый электронный документ, расшифровывают, определяют служебные символы, с их помощью определяют команды и электронную банкноту, подписанную банком, записывают электронную банкноту в ППЗУ персонального криптозащитного комплекса и блокируют до получения определённых команд и выполнения условий банка, содержащихся в полученных командах электронного документа,

принимают в персональный криптозащитный комплекс пользователя электронные банковские векселя, вводят команду пользователя разблокировать электронную банкноту, подписанную банком,

в соответствии с командой пользователя проверяют наличие в ППЗУ электронного банковского векселя и его соответствие условиям банка по сумме, валюте и другим атрибутам, считывают с электронного векселя данные пользователя, включая индивидуальный номер его персонального криптозащитного комплекса, на имя которого выписан электронный вексель,

если электронный вексель отвечает условиям банка, то производят разблокирование электронной банкноты с одновременным уменьшением номинала упомянутого электронного векселя на сумму, соответствующую сумме электронной банкноты, при этом к электронной банкноте добавляют зашифрованную информацию, содержащую данные пользователя, взятые из упомянутого электронного векселя,

подключают к персональному криптозащитному комплексу пользователя посредством терминала носитель и производят передачу электронной банкноты на данный носитель,

производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя,

в банке принимают данную электронную банкноту, дешифруют добавленную к ней информацию, определяют по данной информации счёт пользователя, на котором хранится залоговая сумма под упомянутый электронный вексель, и списывают с него сумму, соответствующую полученной электронной банкноте, заносят электронную банкноту в регистр, и если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя.

54. Способ по п. 53, отличающийся тем, что при совпадении данных пользователя, включая индивидуальный номер его персонального криптозащитного комплекса, в электронном векселя с аналогичными данными в ПЗУ персонального криптозащитного комплекса пользователя производят разблокирование электронной банкноты, включающей в себя номер счёта пользователя, с одновременным уменьшением номинала упомянутого электронного векселя на сумму, соответствующую сумме электронной банкноты, подключают к персональному криптозащитному комплексу пользователя посредством терминала носитель и производят передачу электронной банкноты на данный носитель,

производят транзакцию платежа упомянутой электронной банкнотой с помощью данного носителя,

в банке принимают данную электронную банкноту, определяют по ней счёт пользователя, на котором хранится залоговая сумма под упомянутый электронный вексель, и списывают с него сумму, соответствующую полученной электронной банкноте, заносят электронную банкноту в регистр, и если достоинство электронной банкноты выше, чем сумма платежа, возвращают сдачу на носитель пользователя.

55. Способ осуществления расчётов электронными наличными деньгами с использованием персонального криптозащитного комплекса, при котором

в ПЗУ каждого из персональных криптозащитных комплексов сохраняют копии материнского кода, представляющего собой множество случайных чисел (M1, M2,..., MN), программ шифрования, дешифрования и обработки информации, причем запись производится защищенным способом только в упомянутых персональных криптозащитных комплексах, исключающим возможность записи на другие носители и изменения упомянутых программ,

подключают персональные криптозащитные комплексы друг к другу напрямую либо с использованием канала связи,

устанавливают защищённый сеанс связи с применением персональных криптозащитных комплексов на основе динамически преобразуемого динамического кода, сформированного с помощью одноразового ключа сеанса связи, полученного с использованием случайных чисел, и вводят команду пользователя передать записанные в ППЗУ электронные

наличные деньги определённой валюты и суммы другому абоненту установленного сеанса связи,

проверяют наличие в ППЗУ персонального криптозащитного комплекса записи, соответствующей по форме и содержанию электронным наличным деньгам требуемой валюты,

в случае наличия в ППЗУ упомянутой записи считывают сумму, соответствующую электронным наличным деньгам и сверяют с запрашиваемой суммой,

в случае, если запрашиваемая сумма не превышает считанную сумму, выводят пользователю запрос на его идентификацию,

вводят в персональный криптозащитный комплекс информацию и сверяют ее с хранимыми в персональном криптозащитном комплексе данными, соответствующими идентифицирующими пользователя,

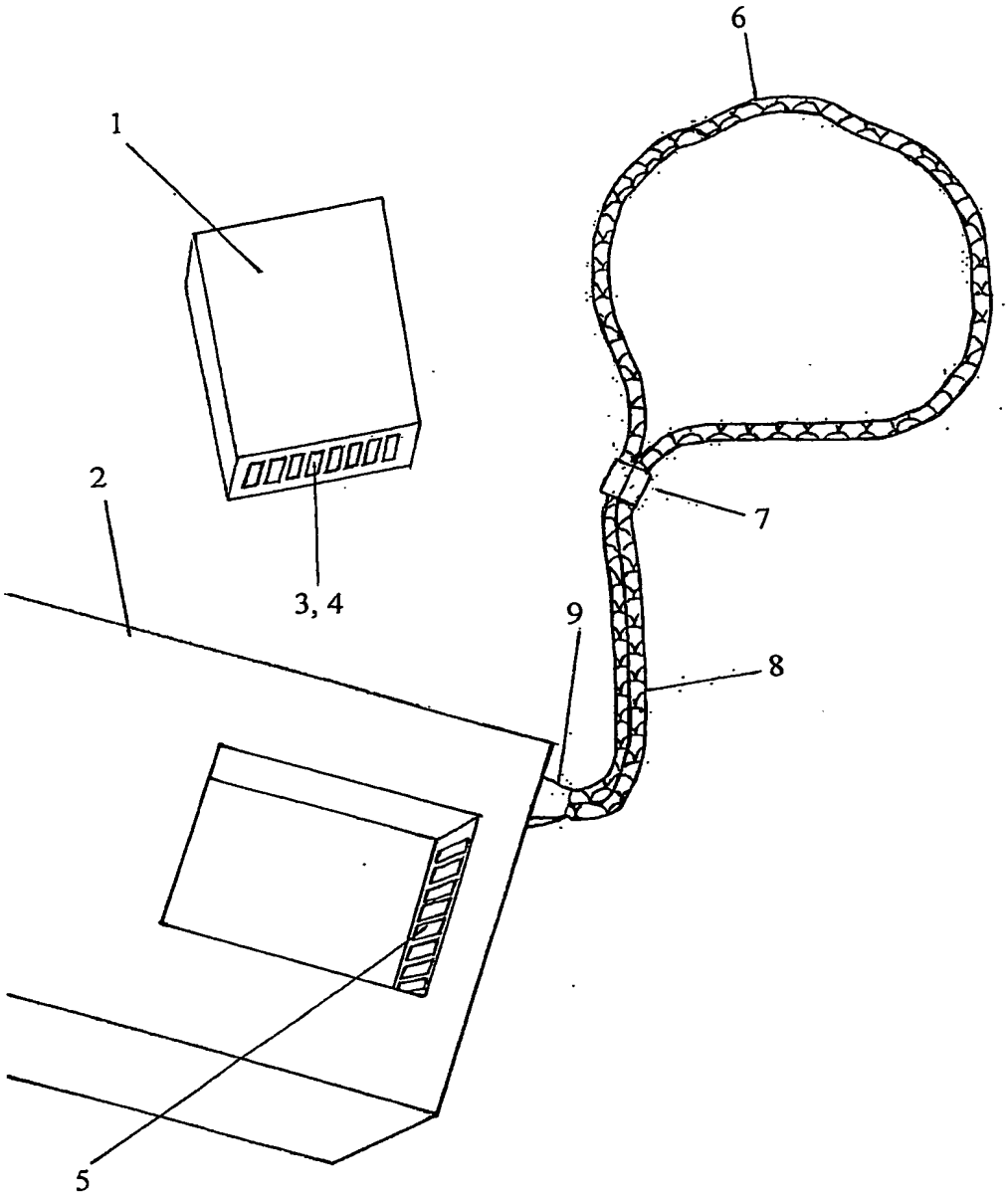
в случае совпадения, с помощью заранее введённой программы обработки информации, формируют типовой электронный документ, содержащий запись электронных денег на запрашиваемую пользователем валюту и сумму,

одновременно производят изменение записи электронных наличных денег, хранимых в ППЗУ, уменьшая их стоимость на передаваемую сумму,

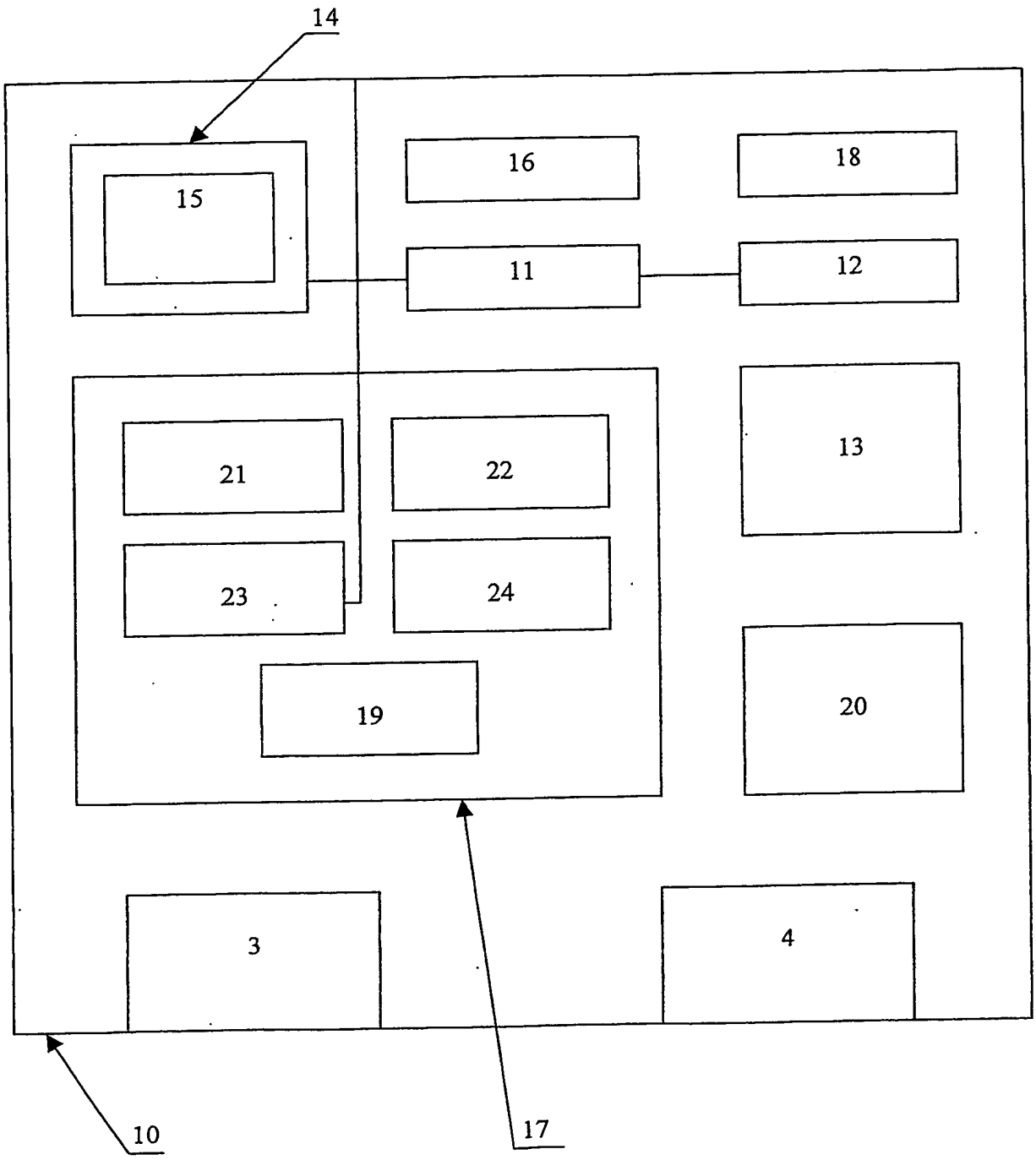
шифруют динамически преобразуемым дочерним кодом упомянутый электронный документ, устанавливают защиту от внесения изменений в зашифрованную информацию и передают зашифрованную информацию в персональный криптозащитный комплекс пользователя, с которым установлен защищённый сеанс связи,

по окончанию успешной передачи электронного документа производят его удаление из ППЗУ,

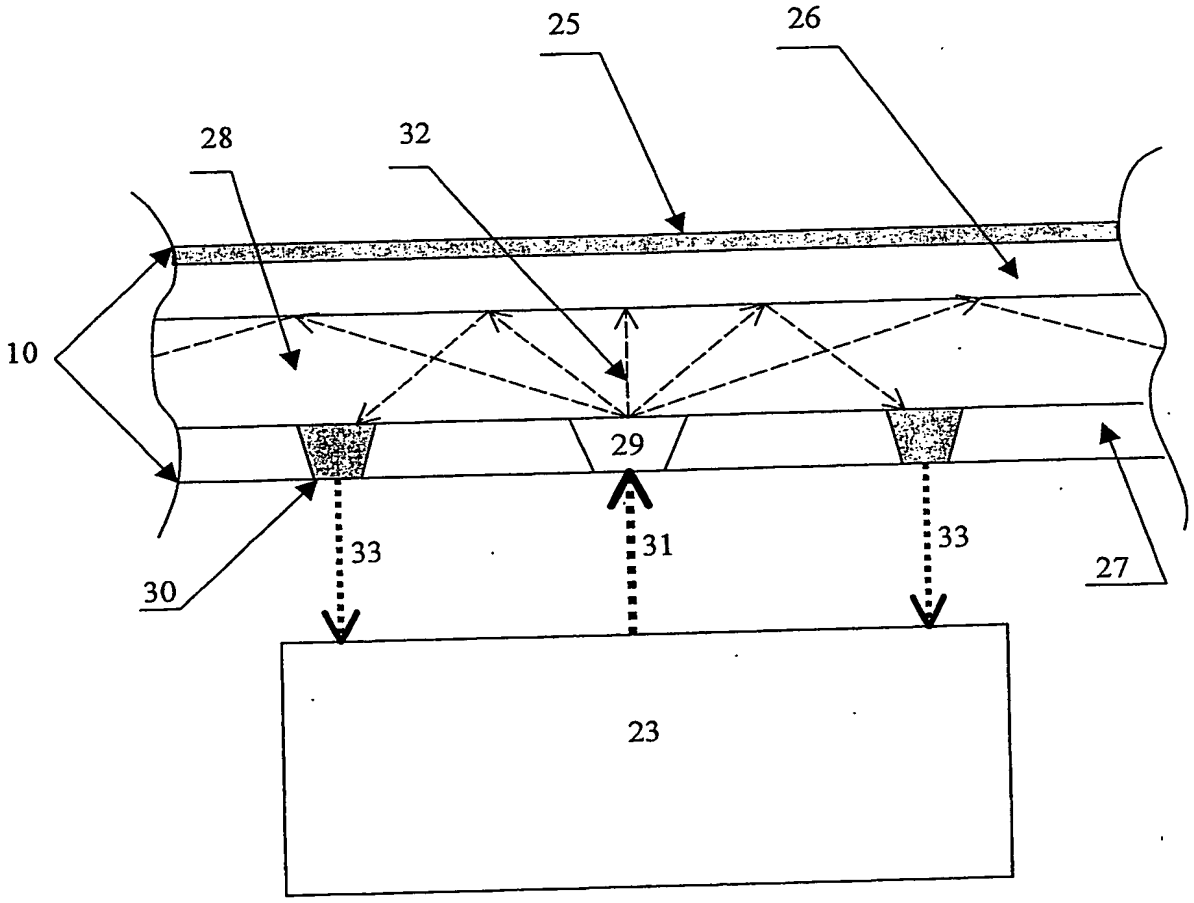
принимают электронный документ, производят дешифрование электронного документа, устанавливают достоверность информации путём проверки на отсутствие искажений в информации и производят запись в ППЗУ, соответствующую по форме и содержанию полученным электронным наличным деньгам.



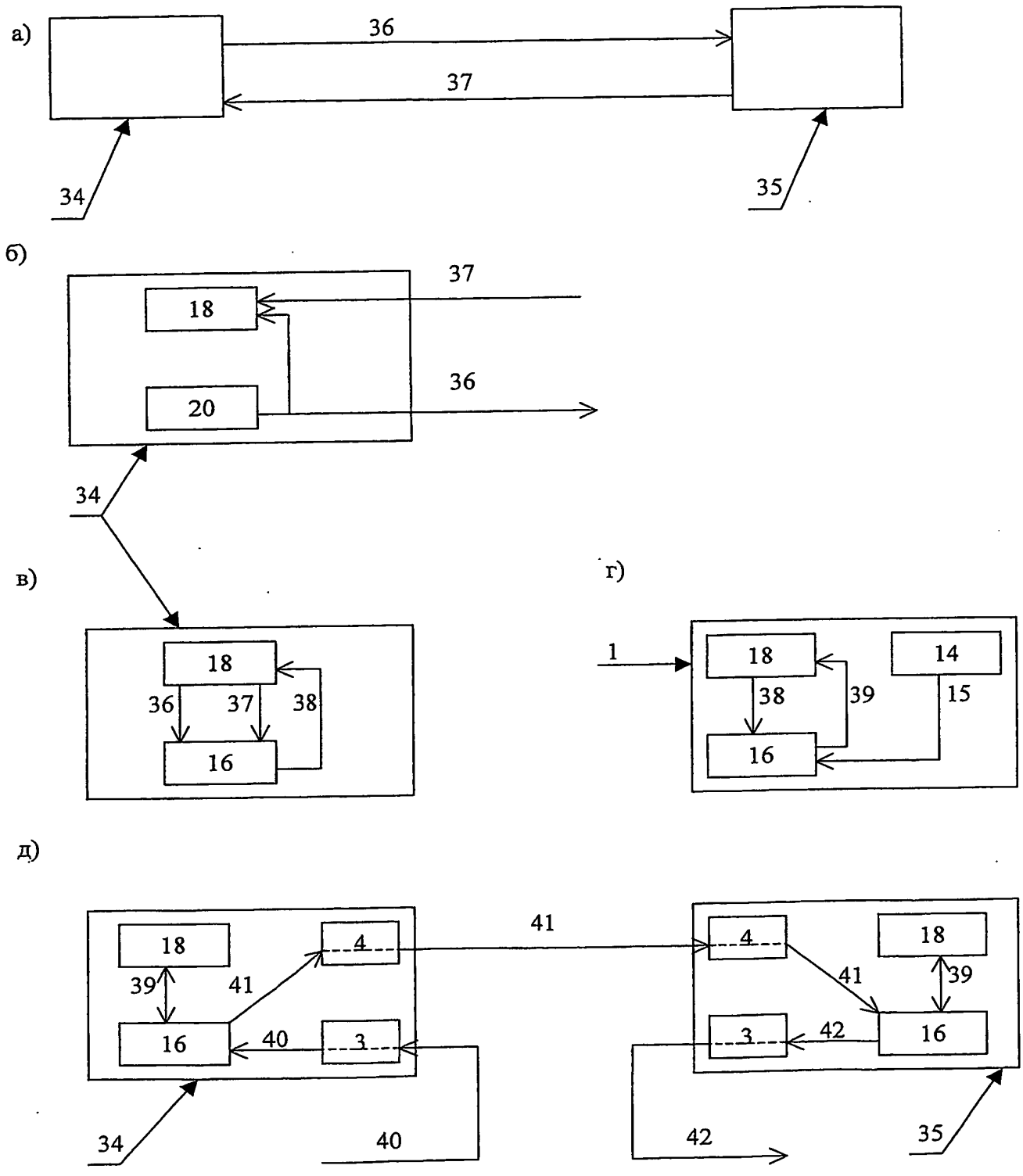
ФИГ. 1



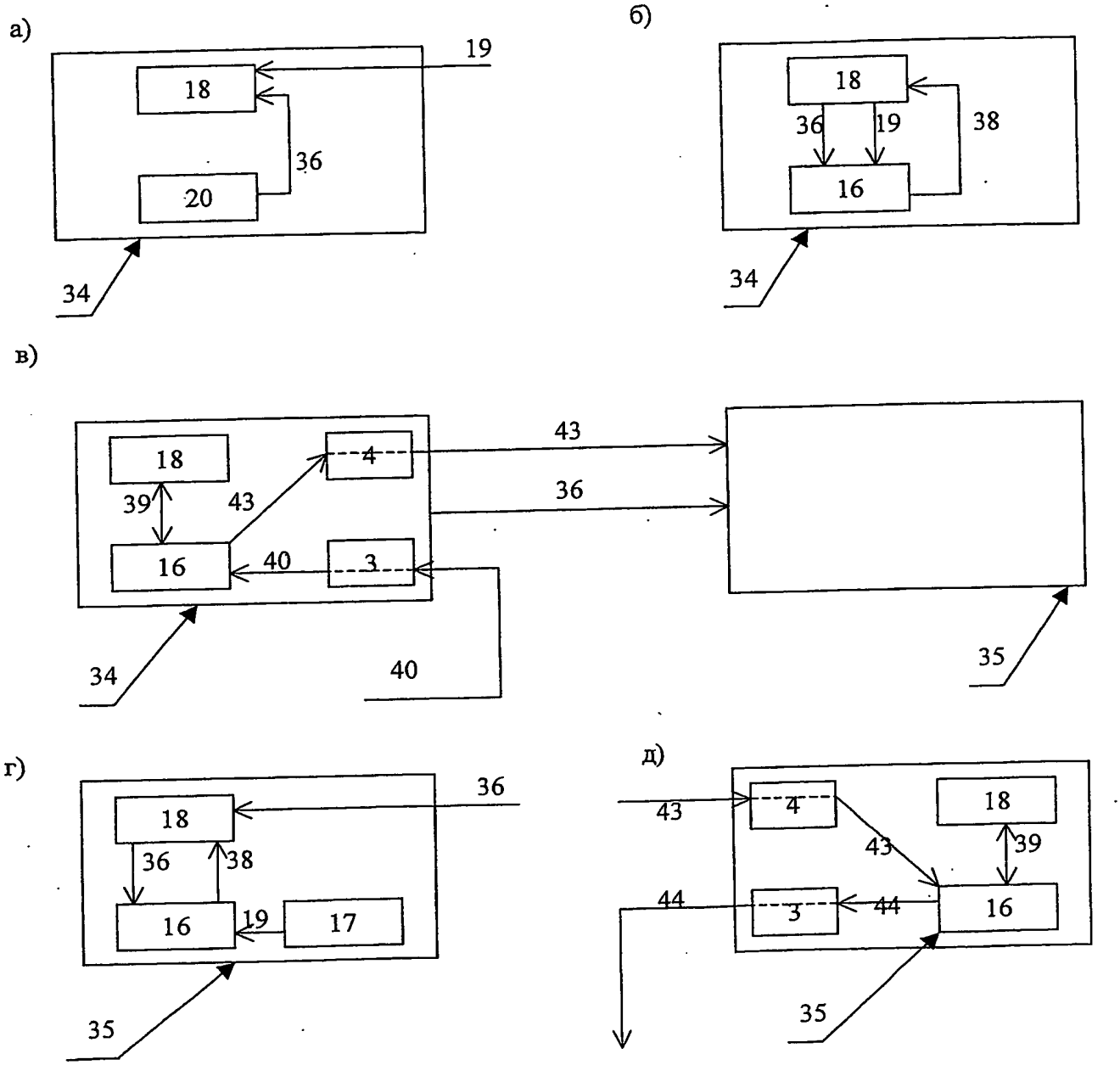
ФИГ. 2



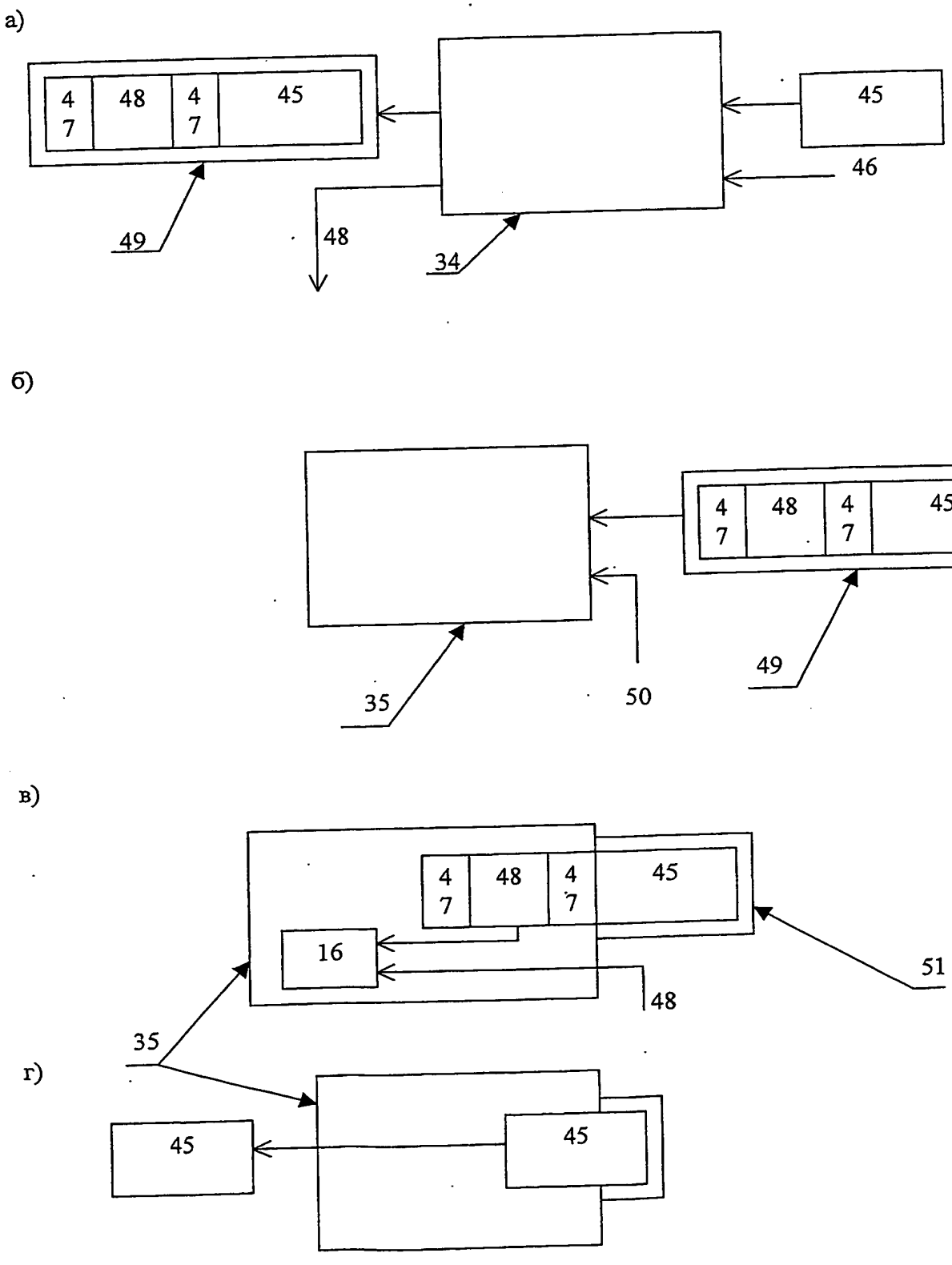
ФИГ. 3


а)
36
37
34
35
б)
37
18
20
36
34
в)
18
36
37
38
16
г)
1
18
14
38
39
15
16
д)
18
4
41
39
41
16
40
3
34
40
4
18
41
39
3
42
16
42
35

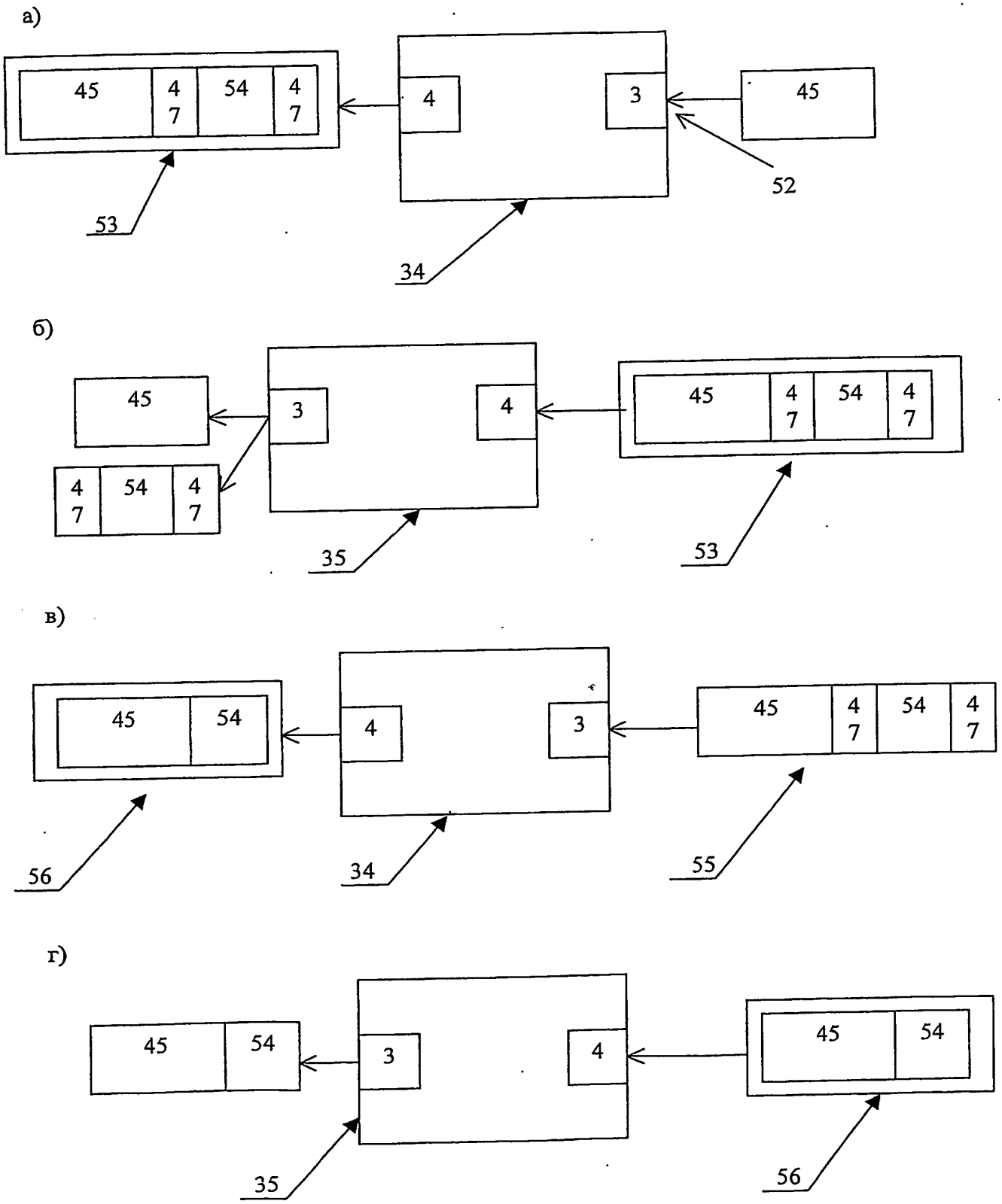
ФИГ. 4


а)
19
18
36
20
34
б)
18
36
19
38
16
34
в)
18
4
43
39
43
36
16
40
3
34
40
35
г)
36
18
36
38
16
19
17
35
д)
43
4
18
43
39
44
3
44
16
35

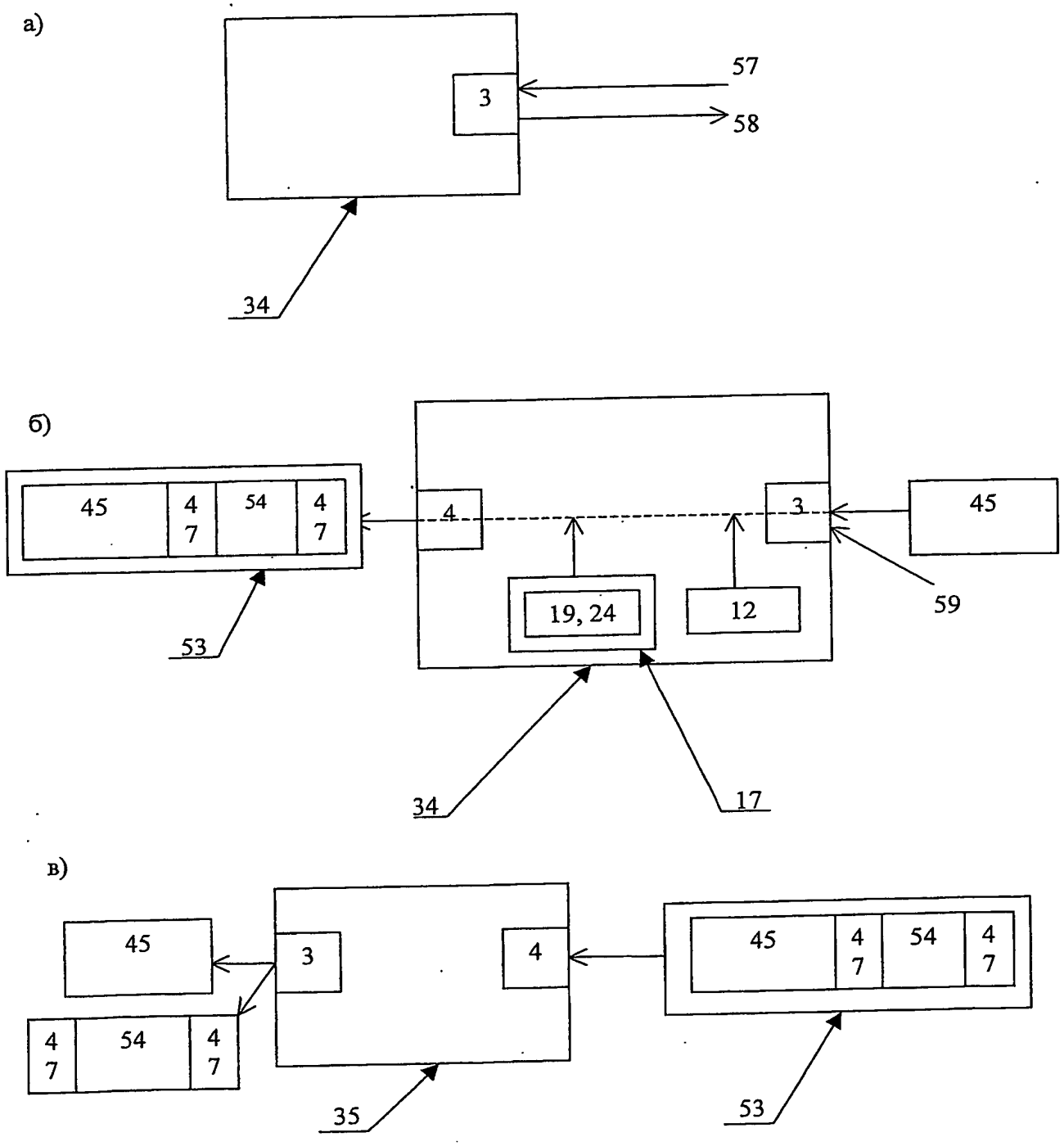
ФИГ. 5


а)
47
48
47
45
45
46
49
48
34
б)
47
48
47
45
35
50
49
в)
47
48
47
45
16
48
51
35
г)
45
45

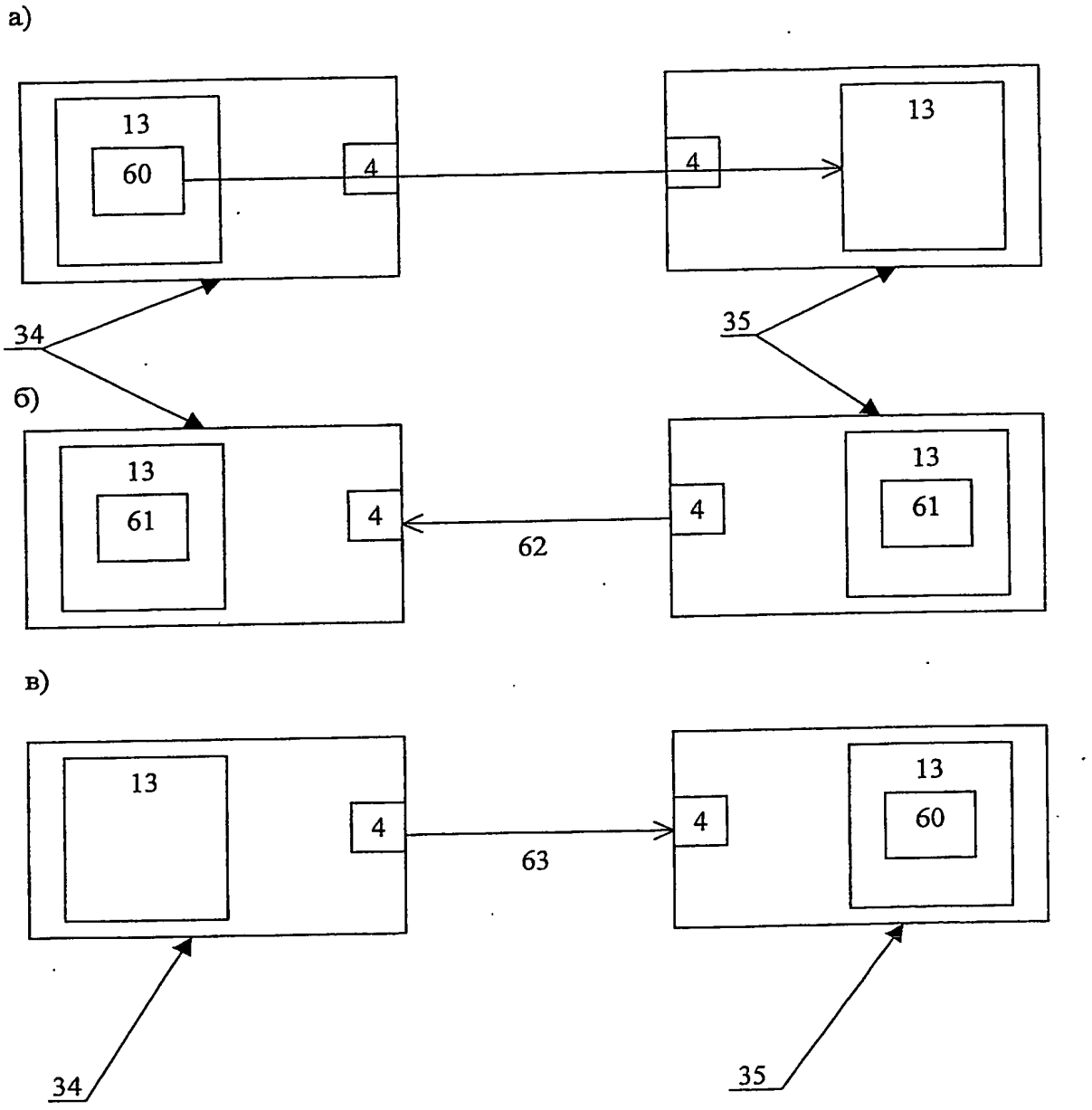
ФИГ. 6


а)
45
47
54
47
4
3
45
53
52
34
б)
45
47
54
47
3
4
45
47
54
47
35
53
в)
45
54
4
3
45
47
54
47
56
34
55
г)
45
54
3
4
45
54
35
56

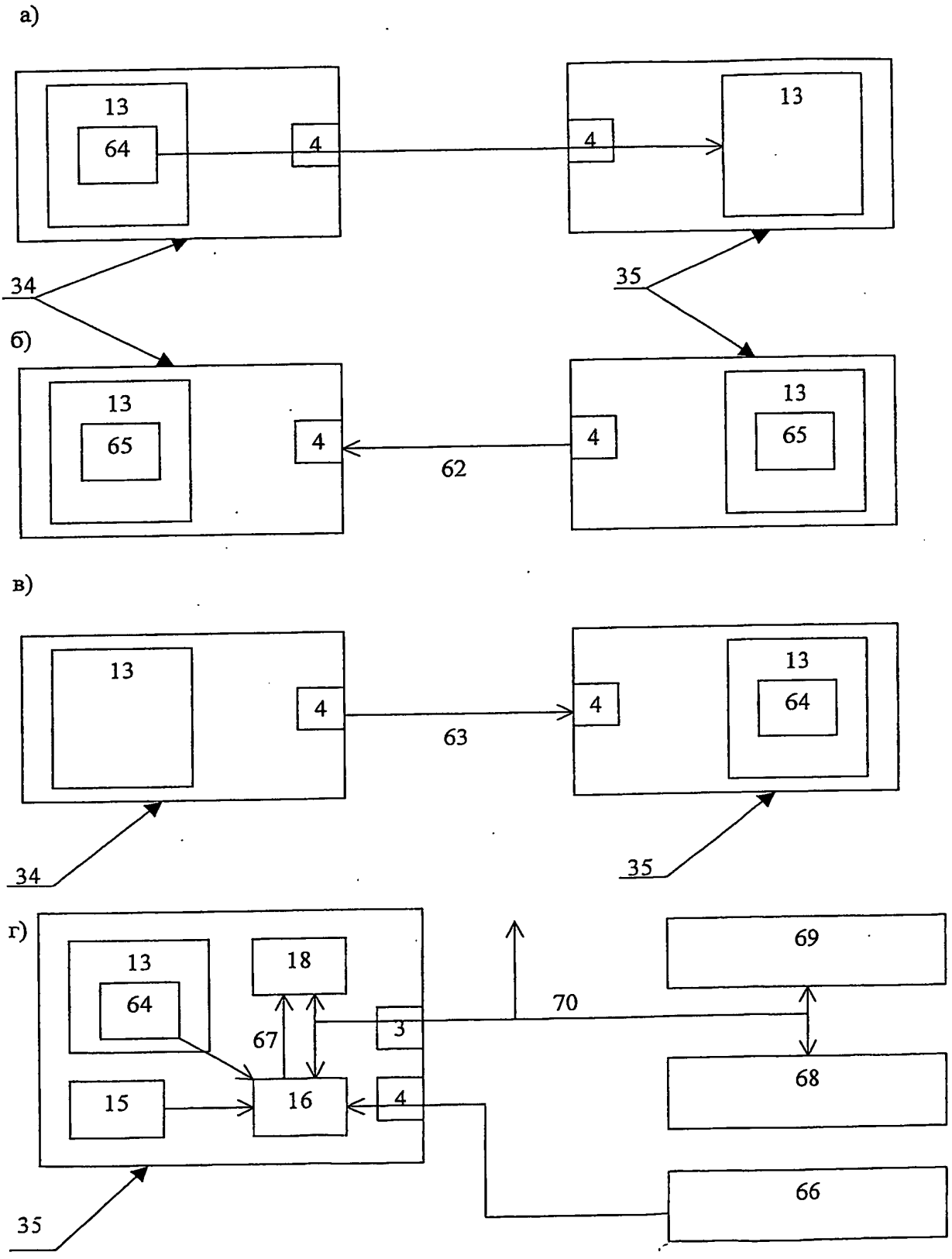
ФИГ. 7


а)
3
57
58
34
б)
45
47
54
47
4
3
45
19, 24
12
59
53
34
17
в)
45
3
4
45
47
54
47
47
54
47
35
53

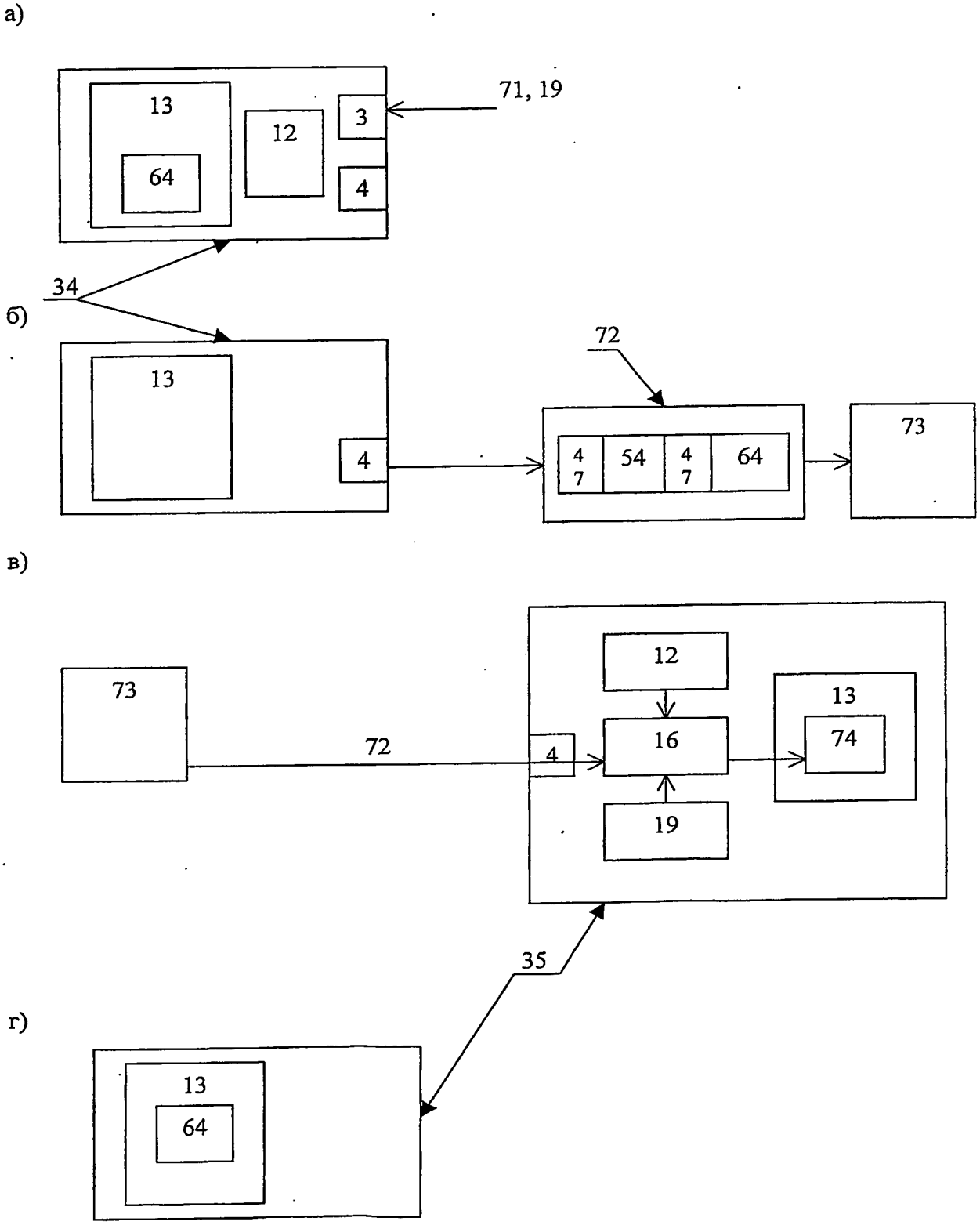
ФИГ. 8



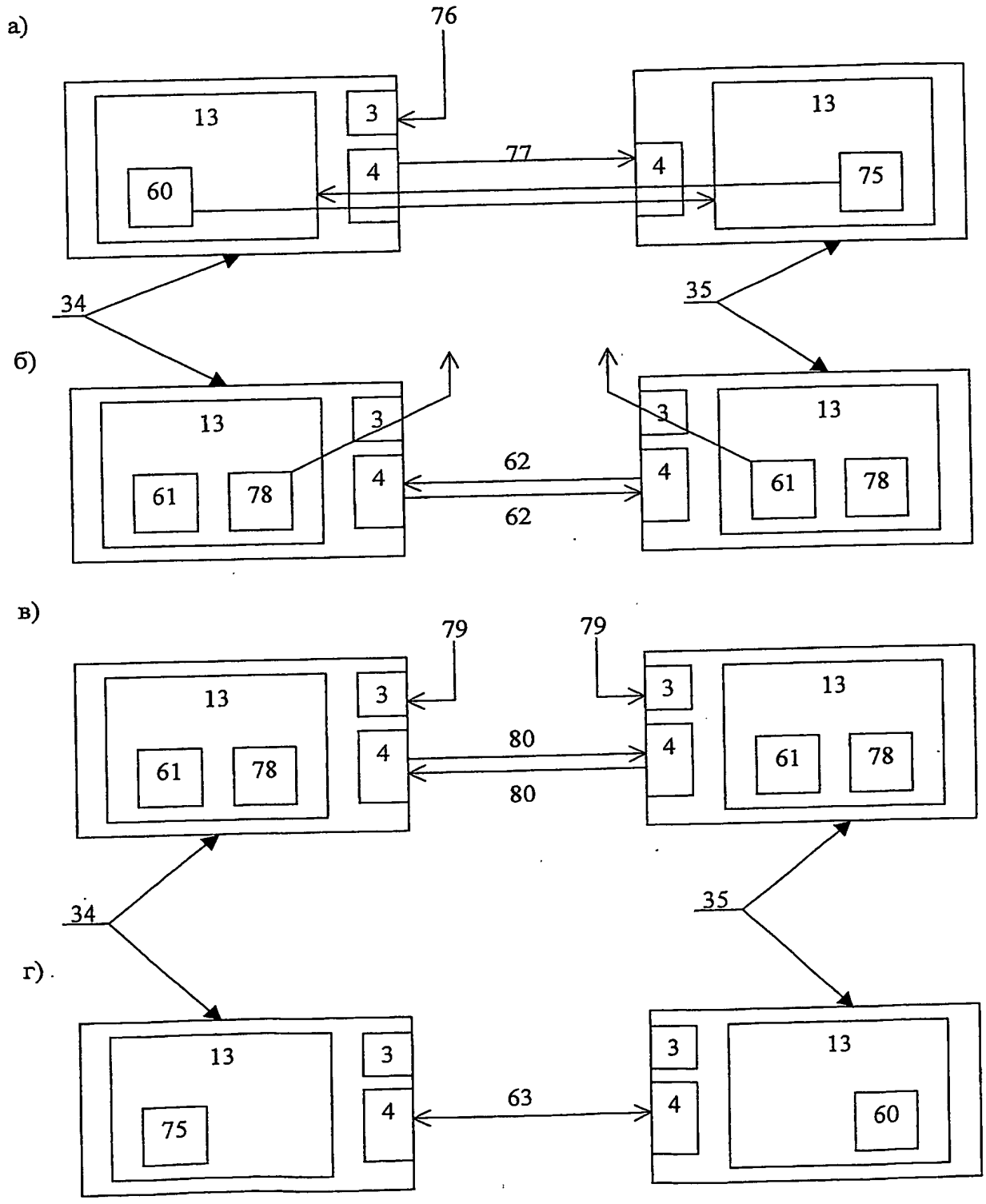
ФИГ. 9


а)
13
64
4
4
13
34
35
б)
13
65
4
4
62
13
65
в)
13
4
63
4
13
64
34
35
г)
13
64
18
67
3
70
69
15
16
4
68
66
35

ФИГ. 10

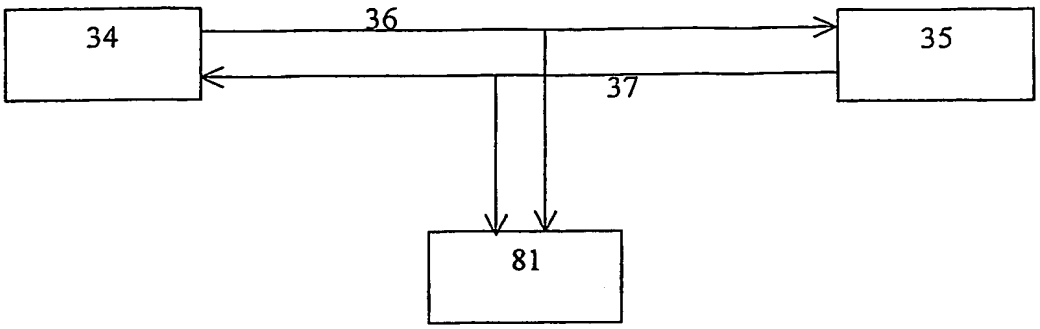

а)
13
64
12
3
4
71, 19
34
б)
13
4
72
47
54
47
64
73
в)
73
72
12
4
16
19
13
74
35
г)
13
64

ФИГ. 11

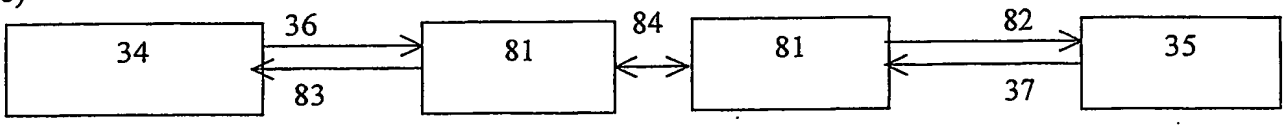

а)
76
13
3
4
60
77
4
13
75
34
35
б)
13
3
4
61
78
62
62
3
4
13
61
78
в)
79
79
13
3
4
61
78
80
80
3
4
13
61
78
34
35
г)
13
3
4
75
63
3
4
13
60

ФИГ. 12

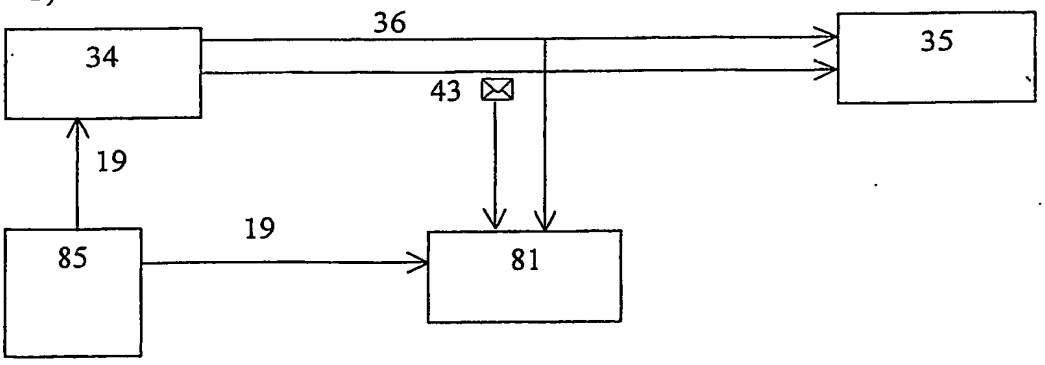
а)



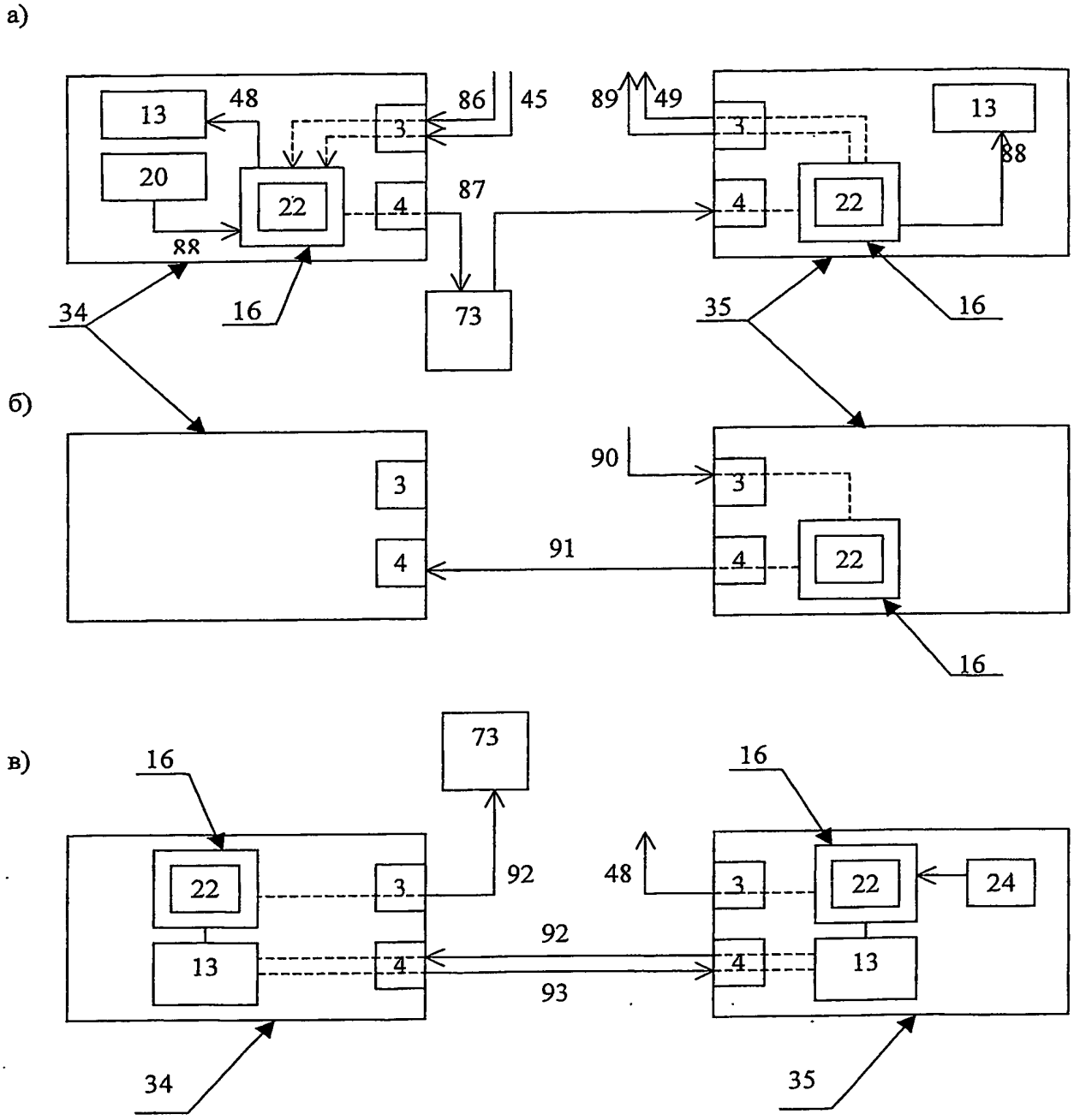
б)



в)



ФИГ. 13


а)
13
48
20
22
3
4
86
45
87
88
34
16
73
89
49
13
88
35
16
б)
3
4
90
91
16
в)
16
73
22
3
92
13
4
48
24
92
93
34
35

ФИГ. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 03/00266

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00, G06F 17/60, G06K 19/073

According to International Patent Classification (IPC) or to both national classification and IPC МПК-7:

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols) МПК-7:

H04L 9/00, 9/06, 9/10, 9/12, 9/28, 9/32, H04K 1/00, G06F 12/00, 12/14, G06F 17/00, 17/60, G06K 19/00, 19/073, G07C 9/00, G09C 1/00, 1/02, 1/06, G07F 19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0295985 A1 (COMPAGNIE GENERALE DES MATIERES NUCLEAIRES (COGEMA)), 21. 12. 1988, Claims 1, 2, figure 1, column 2	43-44 21
Y	RU 2147790 C1 (INTEL CORPORATION) 20.04.2000, claims 1, 3, 5, 8, page 7	19-21
Y	US 5325430 A (TOVEN TECHNOLOGIES INC.), Jun. 28, 1994, п.п.1, 5, 6, 23, 24 формулы	19-21
A	US 5483596 A (PARALON TECHNOLOGIES INC.), Jan. 9, 1996	1-55
A	US 5237611 A (CREST INDUSTRIES INC.), Aug. 17, 1993	1-55
A	RU 2157001 C2 (ZAKRYTOE AKTSIONERNOE OBSCHESTVO "ALKORSOFT"), 27.09.2000	52-55

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 September 2003 (23.09.2003)	**02 October 2003 (02.10.2003)**
Name and mailing address of the ISA/**RU**	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

ОТЧЕТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Международная заявка № PCT/RU 03/00266

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

H04L 9/00, G06F 17/60, G06K 19/073

Согласно международной патентной классификации (МПК-7)

B. ОБЛАСТИ ПОИСКА:

Проверенный минимум документации (система классификации и индексы) МПК-7:

H04L 9/00, 9/06, 9/10, 9/12, 9/28, 9/32, H04K 1/00, G06F 12/00, 12/14, G06F 17/00, 17/60, G06K 19/00, 19/073, G07C 9/00, G09C 1/00, 1/02, 1/06, G07F 19/00

Другая проверенная документация в той мере, в какой она включена в поисковые подборки:

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, поисковые термины):

C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ:

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X Y	EP 0295985 A1 (COMPAGNIE GENERALE DES MATIERES NUCLEAIRES (COGEMA)), 21. 12. 1988, п.п. 1, 2 формулы, фиг. 1, столбец 2	43-44 21
Y	RU 2147790 C1 (ИНТЕЛ КОРПОРЕЙШН), 20. 04. 2000, п.п. 1, 3, 5, 8 формулы, стр. 7	19-21
Y	US 5325430 A (TOVEN TECHNOLOGIES INC.), Jun. 28, 1994, п.п.1, 5, 6, 23, 24 формулы	19-21
A	US 5483596 A (PARALON TECHNOLOGIES INC.), Jan. 9, 1996	1-55
A	US 5237611 A (CREST INDUSTRIES INC.), Aug. 17, 1993	1-55
A	RU 2157001 C2 (ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "АЛКОРСОФТ"), 27. 09. 2000	52-55

☐ последующие документы указаны в продолжении графы C. ☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:

A документ, определяющий общий уровень техники

E более ранний документ, но опубликованный на дату международной подачи или после нее

O документ, относящийся к устному раскрытию, экспонированию и т.д.

P документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета и т.д.

T более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения

X документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень

Y документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории

& документ, являющийся патентом-аналогом

Дата действительного завершения международного поиска: 23 сентября 2003 (23.09.2003)

Дата отправки настоящего отчета о международном поиске: 02 октября 2003 (02. 10. 2003)

Наименование и адрес Международного поискового органа
Федеральный институт промышленной собственности
РФ,123995, Москва, Г-59, ГСП-5, Бережковская наб., 30,1 Факс: 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо:
В. Воропай

Телефон № 240-25-91

Форма PCT/ISA/210 (второй лист)(июль 1998)